**Avaya Solution & Interoperability Test Lab**

# Application notes for OnviSource OnviCord PRO with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Application Enablement Services 6.2 – Issue 1.0

## Abstract


These Application Notes describe the configuration steps required for OnviSource OnviCord PRO to interoperate with Avaya Aura® Communication Manager 6.2 using Avaya Aura® Application Enablement Services 6.2. OnviSource OnviCord PRO is a call recording solution.

In the compliance testing, OnviSource OnviCord PRO used Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to monitor contact center devices on Avaya Aura® Communication Manager, and used the Single Step Conference feature to capture the media associated with the monitored agents for call recording.

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 steps required for OnviSource OnviCord PRO, herein referred to as OnviCord PRO, to interoperate with Avaya Aura® Communication Manager 6.2 using Avaya Aura® Application Enablement Services 6.2. OnviCord PRO is a call recording solution.

OnviCord PRO is software application that provides all the functionality and features required to engage in quality call monitoring and recording. OnviCord PRO delivers simple, browser-based access to a robust tool-set that provides tools needed to manage recorded call information quickly and easily.

OnviCord PRO uses the Device Media and Call Control (DMCC) interface of Avaya Aura® Application Enablement Services to monitor stations and obtain call events. OnviCord PRO also uses the DMCC interface to register DMCC softphones with Avaya Aura® Communication Manger, these softphones are used as recording devices. By combining media redirection from Avaya Aura® Communication Manager with Single Step Conferencing, call recording can be achieved without the use of physical connections to the OnviCord PRO server other than standard network connections.

# 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

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing evaluated the ability of OnviCord PRO to record calls in different call scenarios to ensure good quality audio recordings of calls placed to and from stations on Communication Manager. External calls were made to, and received from the PSTN. The serviceability testing introduced failure conditions to see if OnviCord PRO could properly resume recording calls after each failure recovery.

## 2.2. Test Results

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

- Serviceability testing
  - OnviCord PRO was able to resume recording of calls approximately 3 minutes after disconnecting/reconnecting the Ethernet cable to OnviCord PRO server.
  - OnviCord PRO was able to resume the recording of calls approximately 3 minutes after restoration of network connectivity, and after resets of Avaya Enablement Services.
  - OnviCord PRO was able to resume the recording of calls approximately 5 minutes after restoration of network connectivity, and after resets of Avaya Communication Manager.
- Call Transfers, created two recording files.
- Calls answered by bridged appearances are not recorded; it will only be recorded if the calling endpoint has been configured to be monitored.

## 2.3. Support

Technical support for OnviCord PRO can be obtained by contacting OnviSource at:

- **Phone:** 1-800-388-8402
- **Web:** http://www.onvisource.com/support/
- **Email:** support@onvisource.com

# 3. Reference Configuration

**Figure 1** illustrates the configuration used to test the interoperability of the OnviCord PRO solution with Avaya® Communication Manager and Avaya Aura® Application Enablement Services. Endpoints include Avaya 96xx and 96x1 Series SIP and H.323 IP Telephones, and an Avaya 1416 Digital Telephone. Telephone calls were placed intra-switch (endpoints on the same switch), inter-switch (between sites) over SIP and H.323 Trunks, and outbound/inbound calls to/from the PSTN.

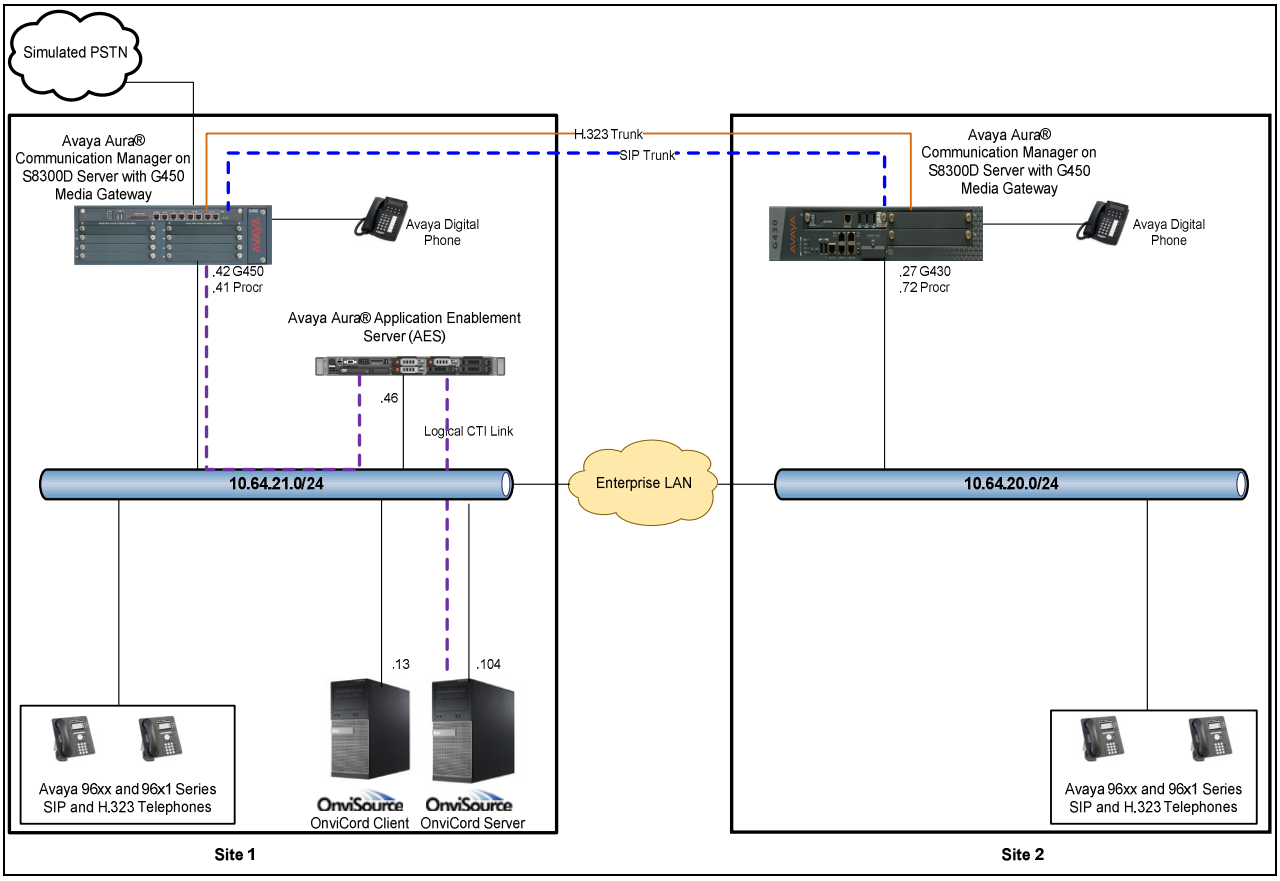



**Figure 1: Test Configuration for OnviCord PRO**

# 4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| **Site 1** | |
| Avaya Aura® Communication Manager on Avaya S8300D Server | R6.2<br>(R016x.02.0.823.0, Patch 20396) |
| G450 Media Gateway | 32.26.0 |
| Avaya Aura® Application Enablement Services on Dell™ PowerEdge™ R610 | 6.2<br>(r6-2-0-18-0 Patch 1) |
| Avaya 1416 Series Digital Phone | - |
| Avaya one-X® Deskphones (SIP) | 2.6.9 (96xx)<br><br>6.2.1 (96x1) |
| Avaya one-X® Deskphones (H.323) | 3.2.0 (96xx)<br><br>6.2.3.13 (96x1) |
| OnviSource OnviCord PRO Server running on Windows 7 Professional 64-bit | 6.2 |
| OnviSource OnviCord PRO Client running on Windows XP Workstation | 6.2 |
| **Site 2** | |
| Avaya Aura® Communication Manager on Avaya S8300D Server | R6.2<br>(R016x.02.0.823.0, Patch 20396) |
| Avaya G430 Media Gateway | 32.26.0 |
| Avaya one-X® Deskphones (SIP) | 2.6.9 (96xx)<br><br>6.2.1 (96x1) |
| Avaya one-X® Deskphones (H.323) | 3.2.0 (96xx)<br><br>6.2.3.13 (96x1) |
| Avaya 1416 Series Digital Phone | - |

# 5. Configure Avaya Aura® Communication Manager

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Communication Manager, refer to the Avaya product documentation, **Reference [1]**.

This section provides the procedures for configuring Avaya Aura® Communication Manager. The procedures include the following areas:

- Verify License
- Administer IP Codec Set
- Administer IP Network Region
- Administer CTI Link
- Administer AE Services
- Administer Stations (DMCC Recording Devices)

## 5.1. Verify License

Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** customer option is set to **y** on **Page 3**.

```
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? y                       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



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

## 5.2. Administer IP Codec Set

Use the **change ip-codec-set n** command, where **n** is the codec set number used for integration with OnviCord PRO. For **Audio Codec**, enter the desired codecs. In the compliance testing, **G.711MU** was used.

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

                          IP Codec Set

    Codec Set: 1

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


     Media Encryption
 1: none
```

## 5.3. Administer IP Network Region

Use the **change ip-network-region n** command, where **n** is the network region number to be used with the OnviCord PRO recording solution. Set the **Codec Set** field to the codec set value administered in **Section 5.2**.

```
change ip-network-region 1                                      Page   1 of  20
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

## 5.4. Administer CTI Link

Add a CTI link using the **add cti-link n** command where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                                  Page   1 of   3
                                   CTI LINK
 CTI Link: 1
Extension: 58001
     Type: ADJ-IP
                                                                     COR: 1
     Name: TSAPI Link 1 - AES_21_46
```

## 5.5. Administer AE Services

An AE Services link must be established between Communication Manager and Application Enablement Services. Use the command **change node-names ip** and enter the node **Name** and **IP Address** for Application Enablement Services in this case **10.64.21.46**. Take a note of the **procr** IP Address **10.64.21.41**, it will needed in **Section 6.3**.

```
change node-names ip                                            Page   1 of   2
                                 IP NODE NAMES
    Name              IP Address
AES_21_46           10.64.21.46
CM_10_67            10.64.10.67
CM_20_40            10.64.20.40
CM_20_72            10.64.20.72
CM_21_40            10.64.21.40
IPO_21_64           10.64.21.64
IPO_21_67           10.64.21.67
IPO_21_68           10.64.21.68
SM_10_62            10.64.10.62
SM_21_31            10.64.21.31
SM_50_31            10.64.50.31
default             0.0.0.0
faxserver           10.64.21.200
procr               10.64.21.41
```

Use the **change ip-services** command. On Page 1, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. During the compliance test, the **Local Node** field is set to the processor Ethernet interface **procr** which is the IP address of Communication Manager in Site 1 as shown in **Figure 1**. The default port **8765** was utilized for the Local Port field.

```
change ip-services                                          Page   1 of   3

                                  IP SERVICES
 Service      Enabled     Local        Local       Remote      Remote
  Type                    Node         Port        Node        Port
AESVCS         y      procr            8765
```

On **Page 3**, enter the hostname of the Application Enablement Services server for the **AE Services Server** field. Enter an alpha-numeric password for the **Password** field and set the **Enabled** field to **y**. The same password will be configured on the Application Enablement Services server in **Section 6.3**.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       AES_21_46         xxxxxxxxxxxxx         y        in use
```

## 5.6. Administer Stations (DMCC Recording Devices)

This section provides the steps required for configuring stations on Communication Manager that will function as recording devices for OnviCord PRO.

Use the **add station n** command where **n** is an available extension. Set the **Type** to a recommended value for DMCC, in this case, **9630**, and specify the **Name**. Specify the **Security Code**, which will be used in **Section 7.3.2**. Set IP SoftPhone to **y**.

```
change station 53031                                          Page   1 of   5
                                     STATION

Extension: 53031                        Lock Messages? n               BCC: 0
     Type: 9630                         Security Code: 123456           TN: 1
     Port: S00002                     Coverage Path 1:                 COR: 1
     Name: DMCC Softphone 1           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: 53031
           Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 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
```

Repeat this step for each DMCC recording device required for the configuration. During compliance testing, 6 DMCC recording devices were administered to be able to record up to 6 calls simultaneously.

# 6. Configure Avaya Aura® Application Enablement Services

Application Enablement Services enables Computer Telephony Interface (CTI) applications to monitor and control telephony resources on Communication Manager. The Application Enablement Services server receives requests from CTI applications, and forwards them to Communication Manager. Conversely, the Application Enablement Services server receives responses and events from Communication Manager and forwards them to the appropriate CTI applications.

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

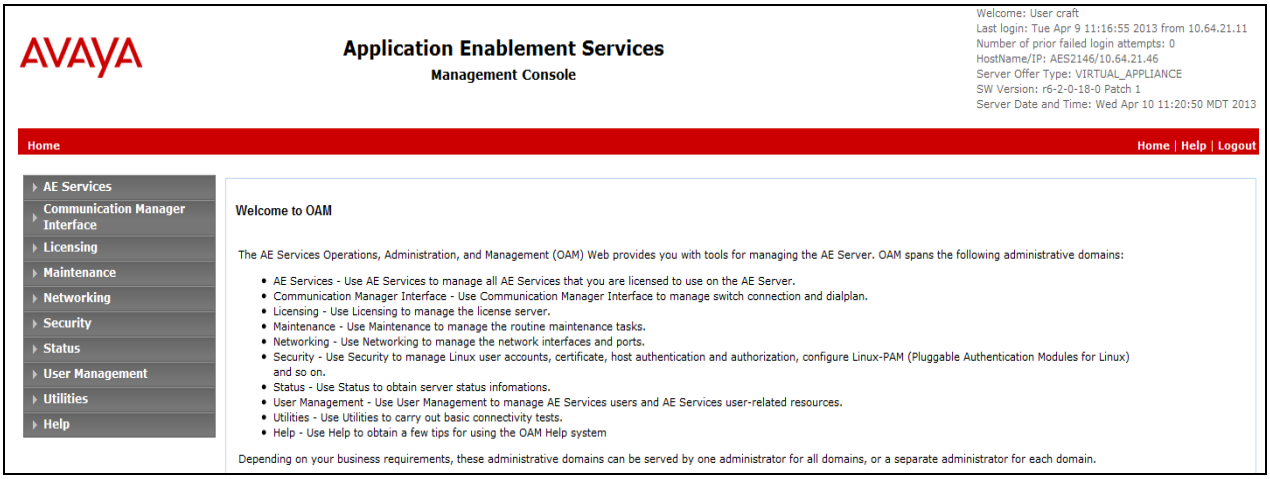
- Launch OAM Interface
- Verify License
- Administer Switch Connection
- Administer TSAPI (Telephony Services API) link
- Restart TSAPI Service
- Obtain Tlink Name
- Administer CTI User
- Enable CTI User
- Administer DMCC Unencrypted Port

## 6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL **https://ip-address** in an Internet browser window, where the **ip-address** is the IP address of the Application Enablement Services server.

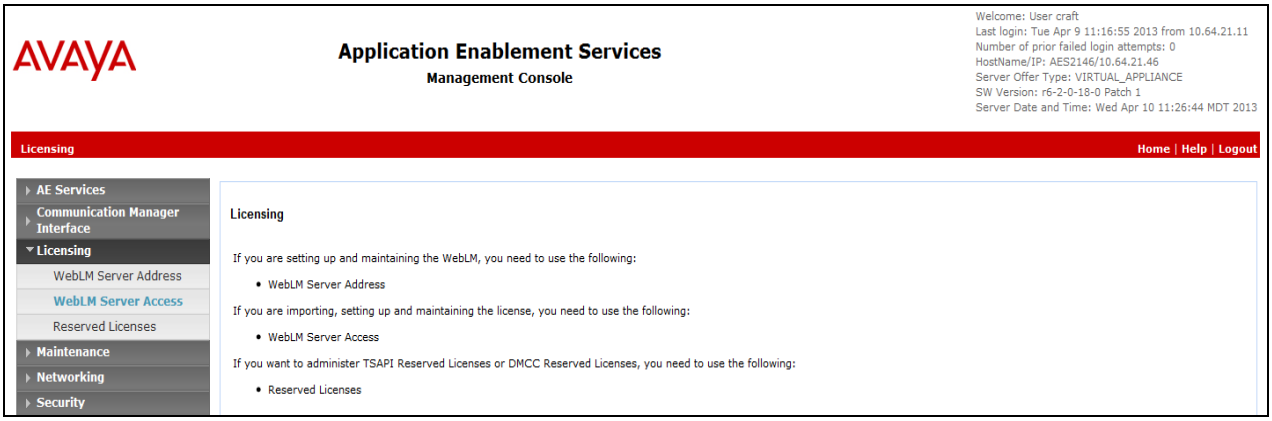
The **Please login here** screen is displayed. Log in using the appropriate credentials.

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



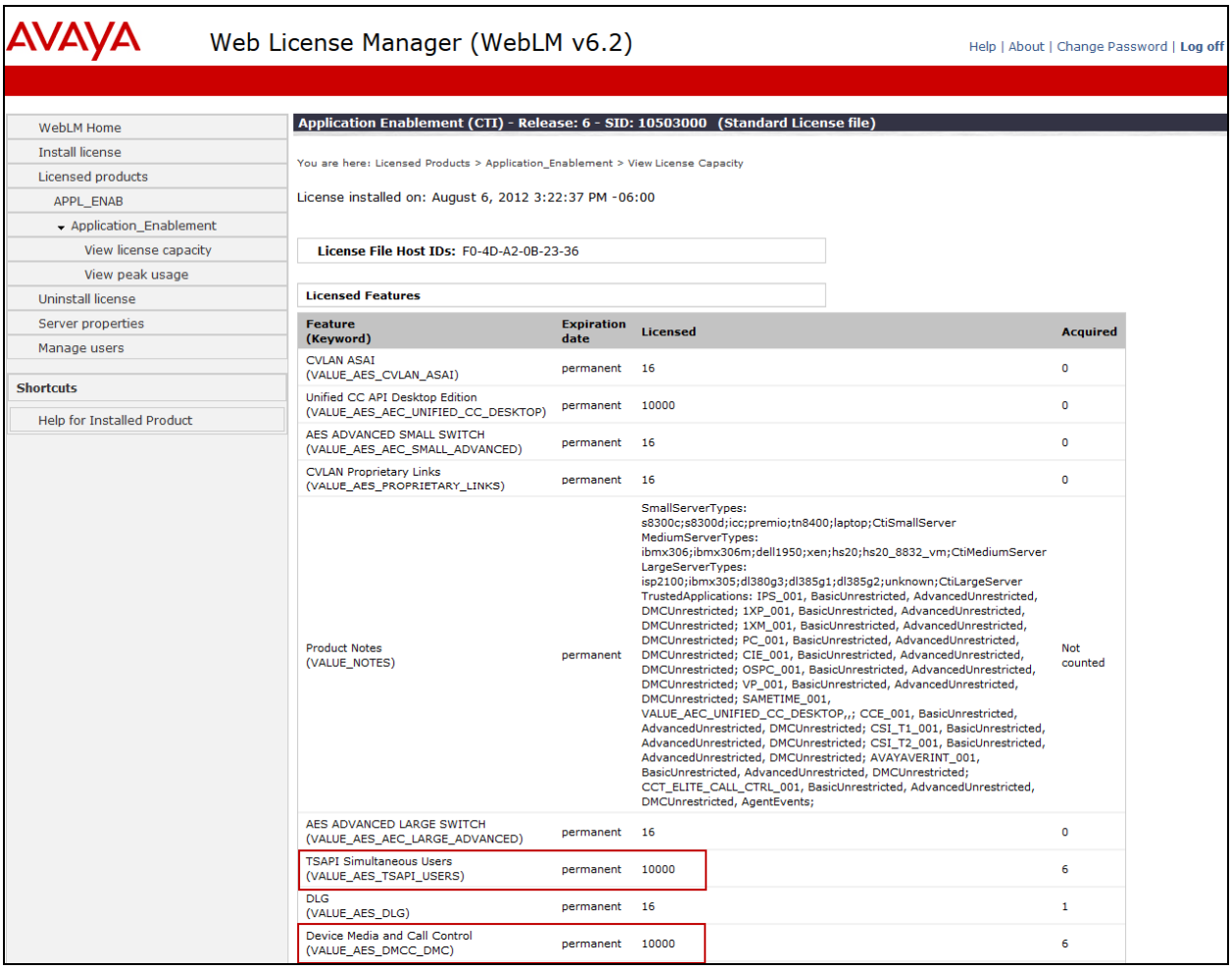

## 6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in with the appropriate credentials.



The **Web License Manager** screen below is displayed. Select **Licensed products →APPL_ENAB → Application_Enablement** in the left pane, to display the **Licensed Features** in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for agent station extension and skill group monitors via DMCC, and the DMCC license is used for the virtual IP softphones.

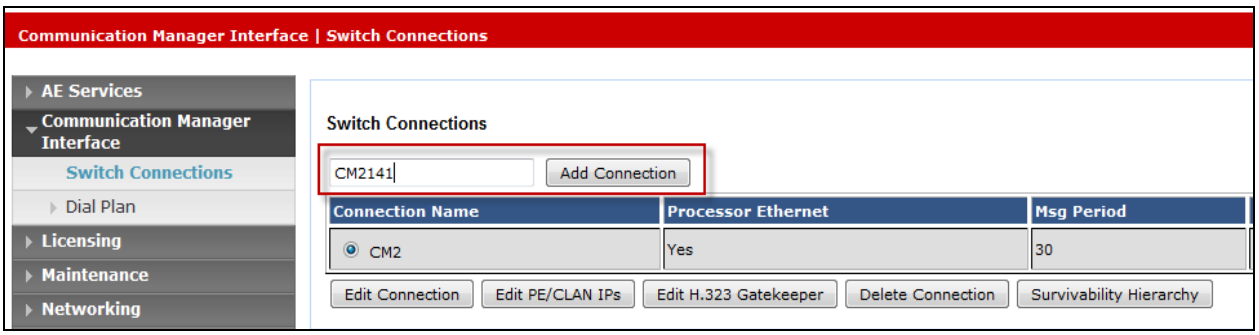



| Feature (Keyword) | Expiration date | Licensed | Acquired |
|---|---|---|---|
| CVLAN ASAI (VALUE_AES_CVLAN_ASAI) | permanent | 16 | 0 |
| Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP) | permanent | 10000 | 0 |
| AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED) | permanent | 16 | 0 |
| CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS) | permanent | 16 | 0 |
| Product Notes (VALUE_NOTES) | permanent | SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; | Not counted |
| AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED) | permanent | 16 | 0 |
| TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS) | permanent | 10000 | 6 |
| DLG (VALUE_AES_DLG) | permanent | 16 | 1 |
| Device Media and Call Control (VALUE_AES_DMCC_DMC) | permanent | 10000 | 6 |

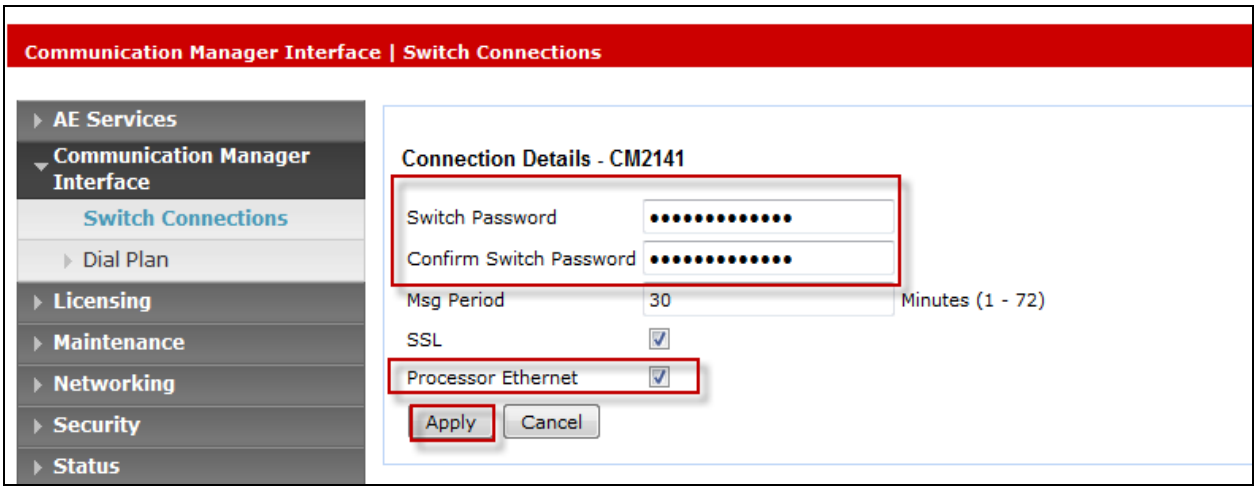
## 6.3. Administer Switch Connection

This section provides the steps required for configure a **Switch Connection**. A Switch Connection defines a connection between Application Enablement Services and Communication Manager.

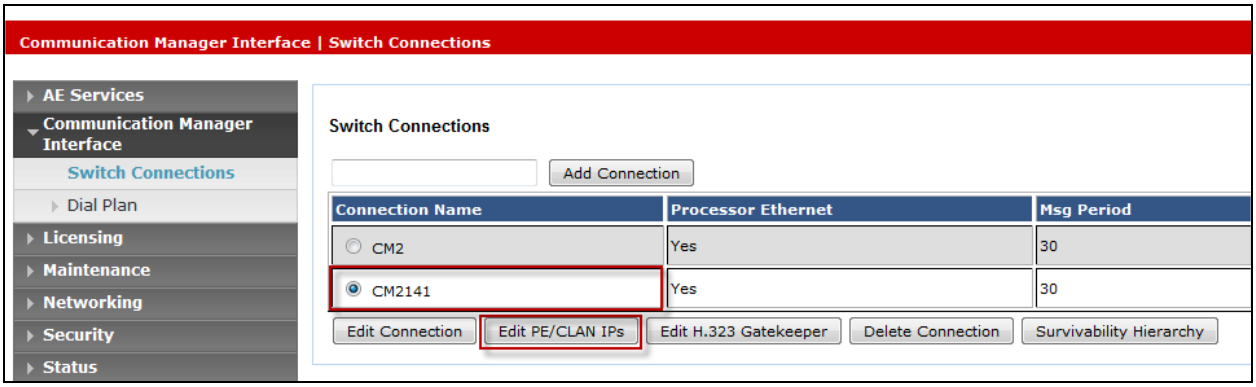
From the left menu, select **Communication Manager Interface → Switch Connections**. Enter a descriptive name, in this case **CM2141**, for the **Switch Connection** and click **Add Connection**.



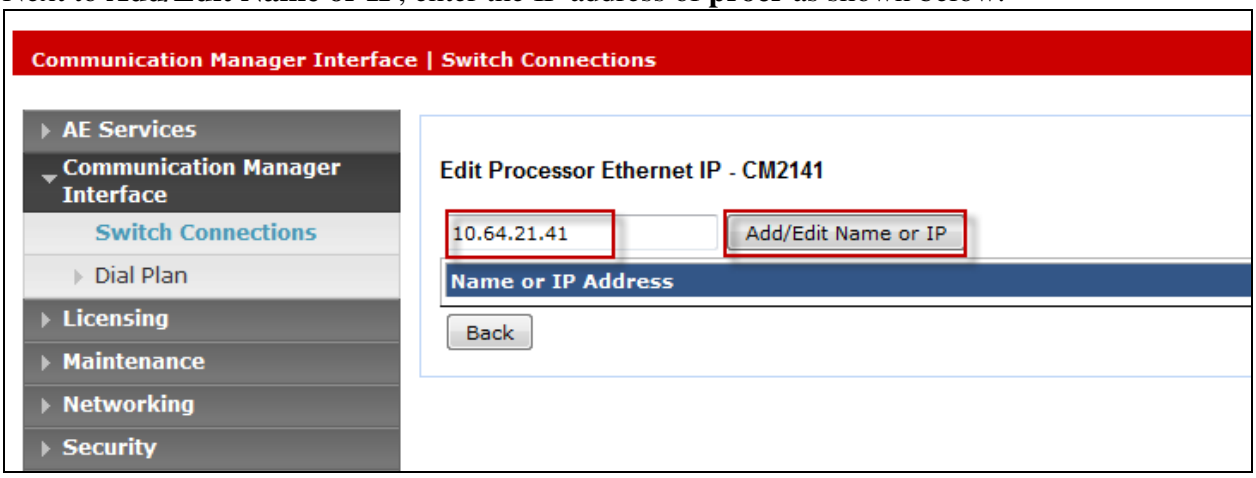

The **Connection Details – CM2141** screen is displayed. For the **Switch Password** and **Confirm Switch Password** fields; enter the password that was administered in Communication Manager using the IP Services form in **Section 5.5**. **Processor Ethernet** fields need to be checked. Retain the default value in the remaining fields. Click on **Apply**.



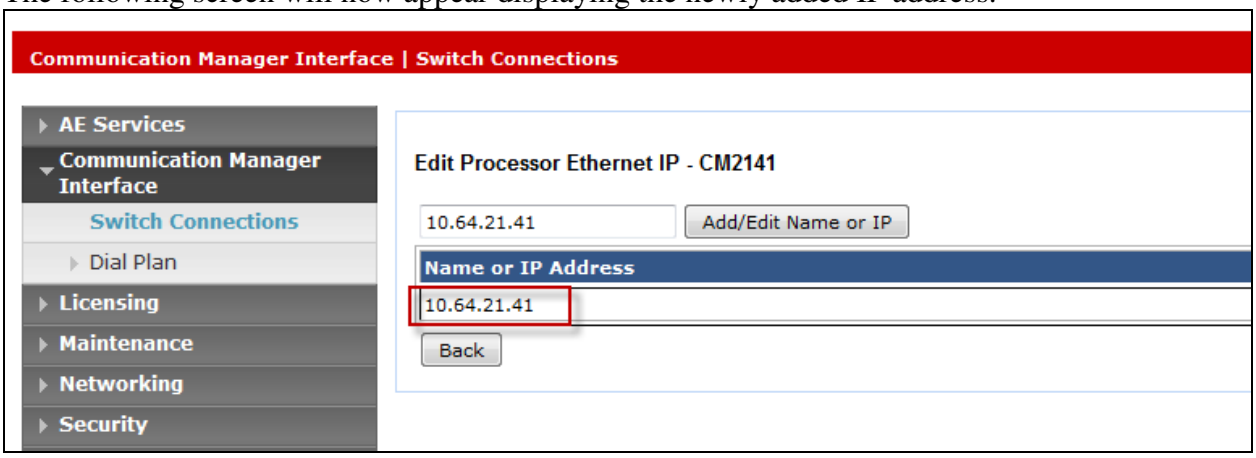
The following screen will be shown displaying the newly added switch connection, select the connection and click on **Edit PE/CLAN IPs** in order to specify the IP address of **procr**, as noted in **Section 5.5**.




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



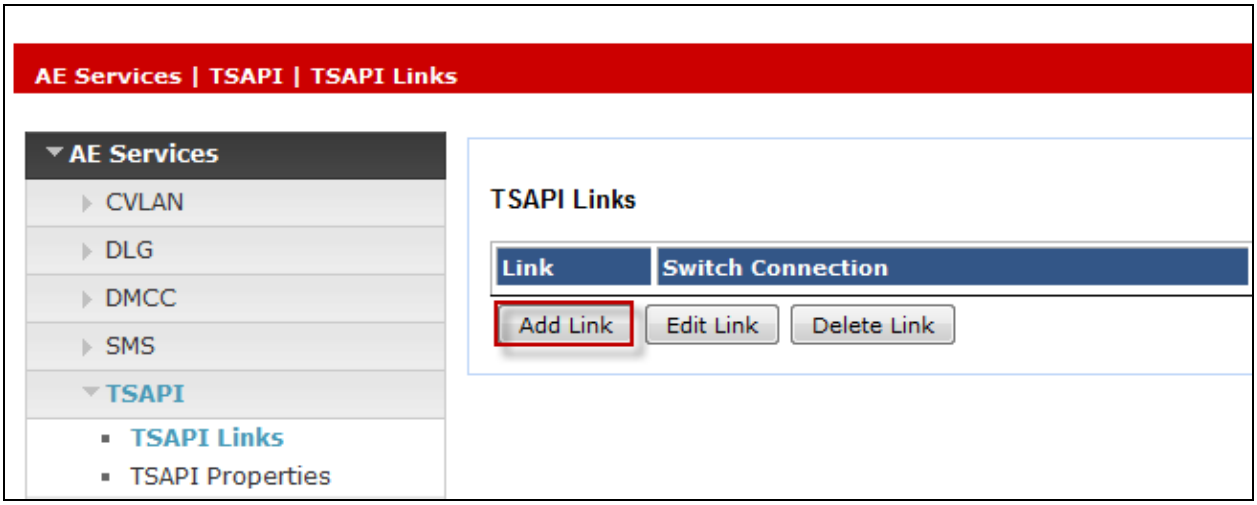

The following screen will now appear displaying the newly added IP address.



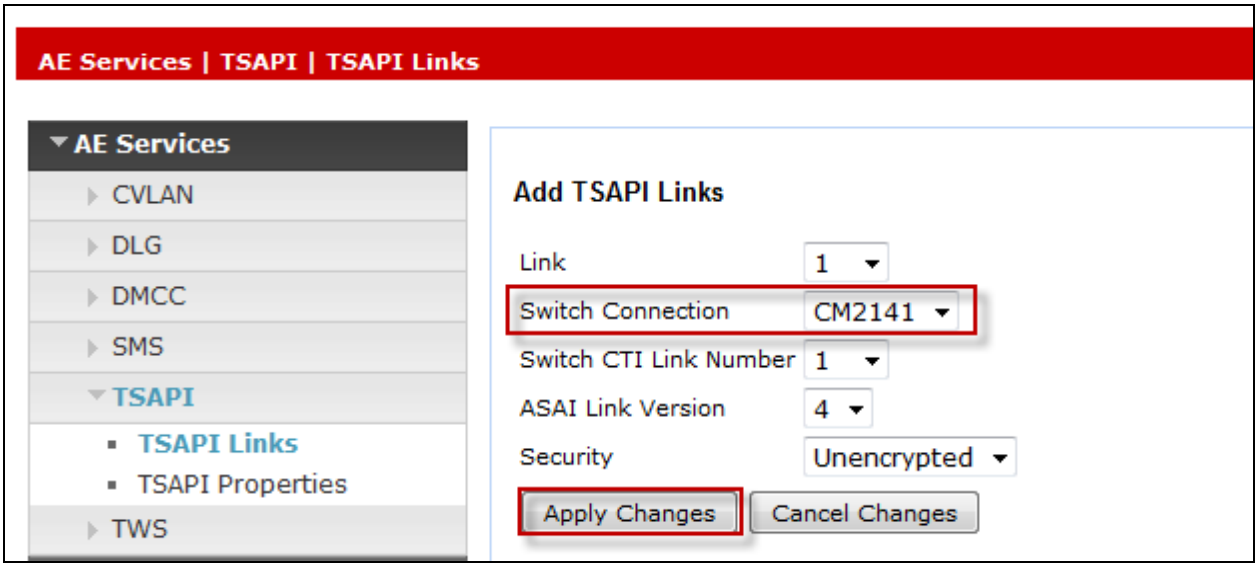

**Note:** Repeat the same steps as above for **Edit H.323 Gatekeeper** adding **procr** IP address.

## 6.4. Administer TSAPI Link

To administer a TSAPI link, select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console**. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

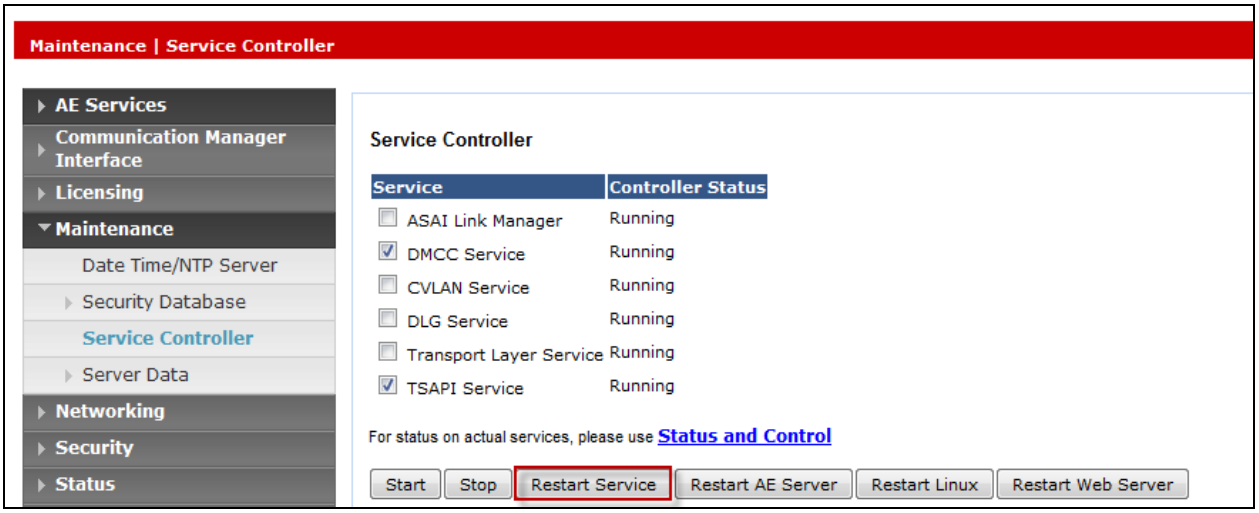



Configure the **TSAPI Link** using the newly configured **Switch Connection** as shown below and click **Apply Changes**.



## 6.5. Restart TSAPI Service

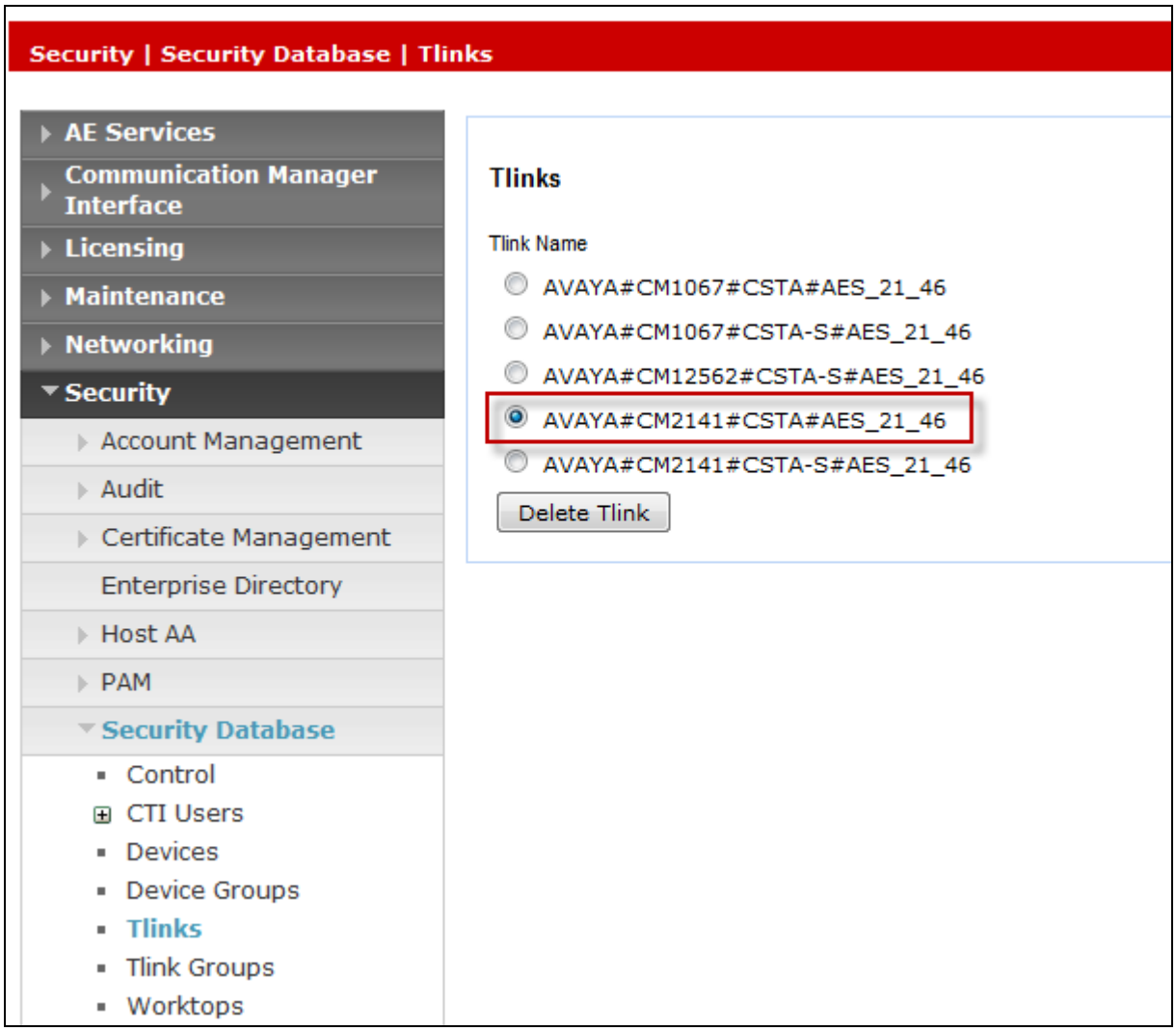
Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service**, and click **Restart Service**.



## 6.6. Obtain Tlink Name

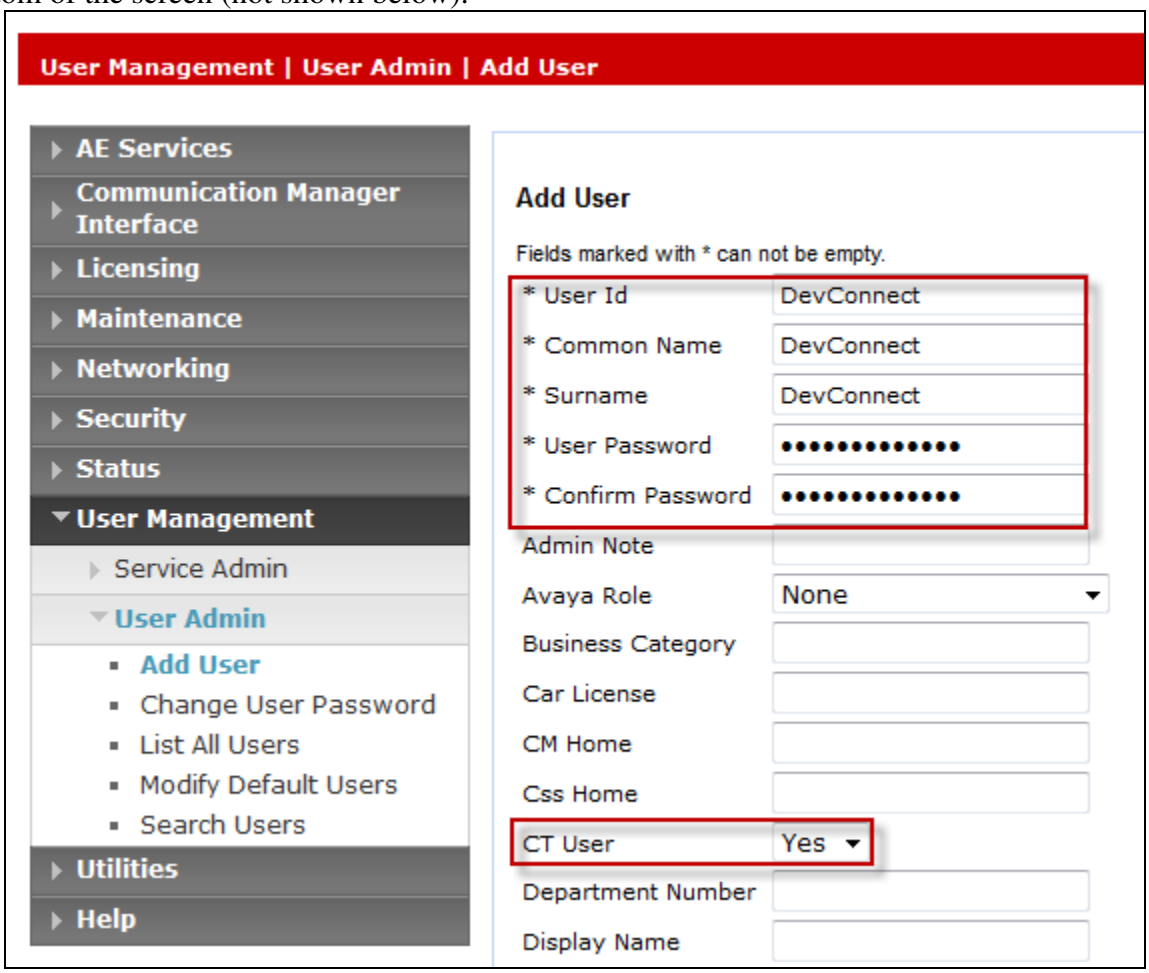
Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring OnviCord PRO.

In this case, the associated Tlink name is **AVAYA#CM2141#CSTA#AES_21_46**. Note the use of the switch connection **CM2141** from **Section 6.3** as part of the Tlink name.



## 6.7. Administer CTI User

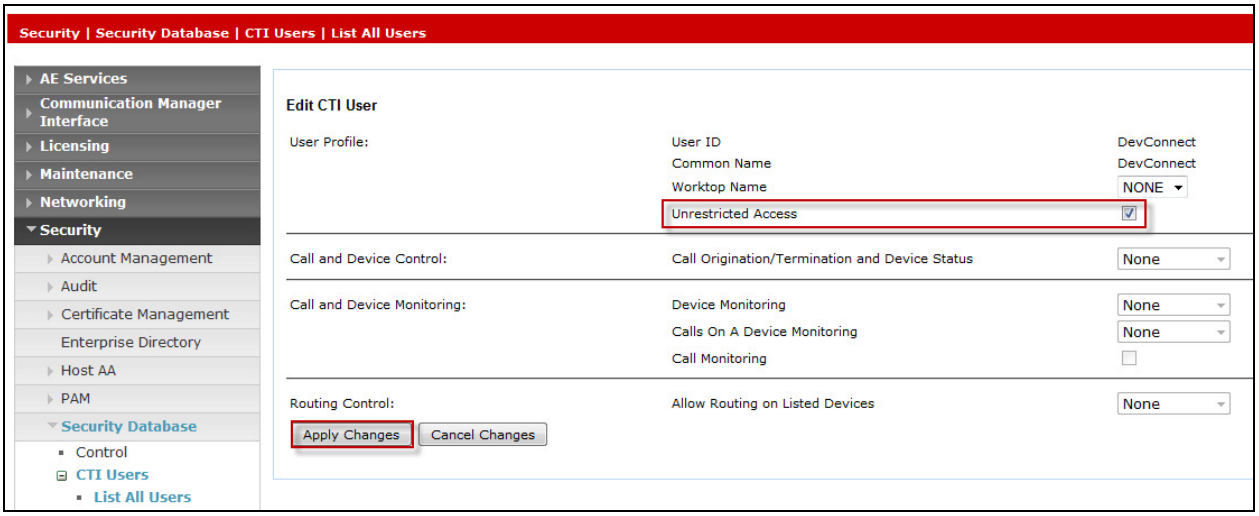
In this section a CTI user is configured for OnviCord PRO to communicate with Application Enablement Services. Select **User Management → User Admin → Add User** from the left pane to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **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).



## 6.8. Enable CTI User

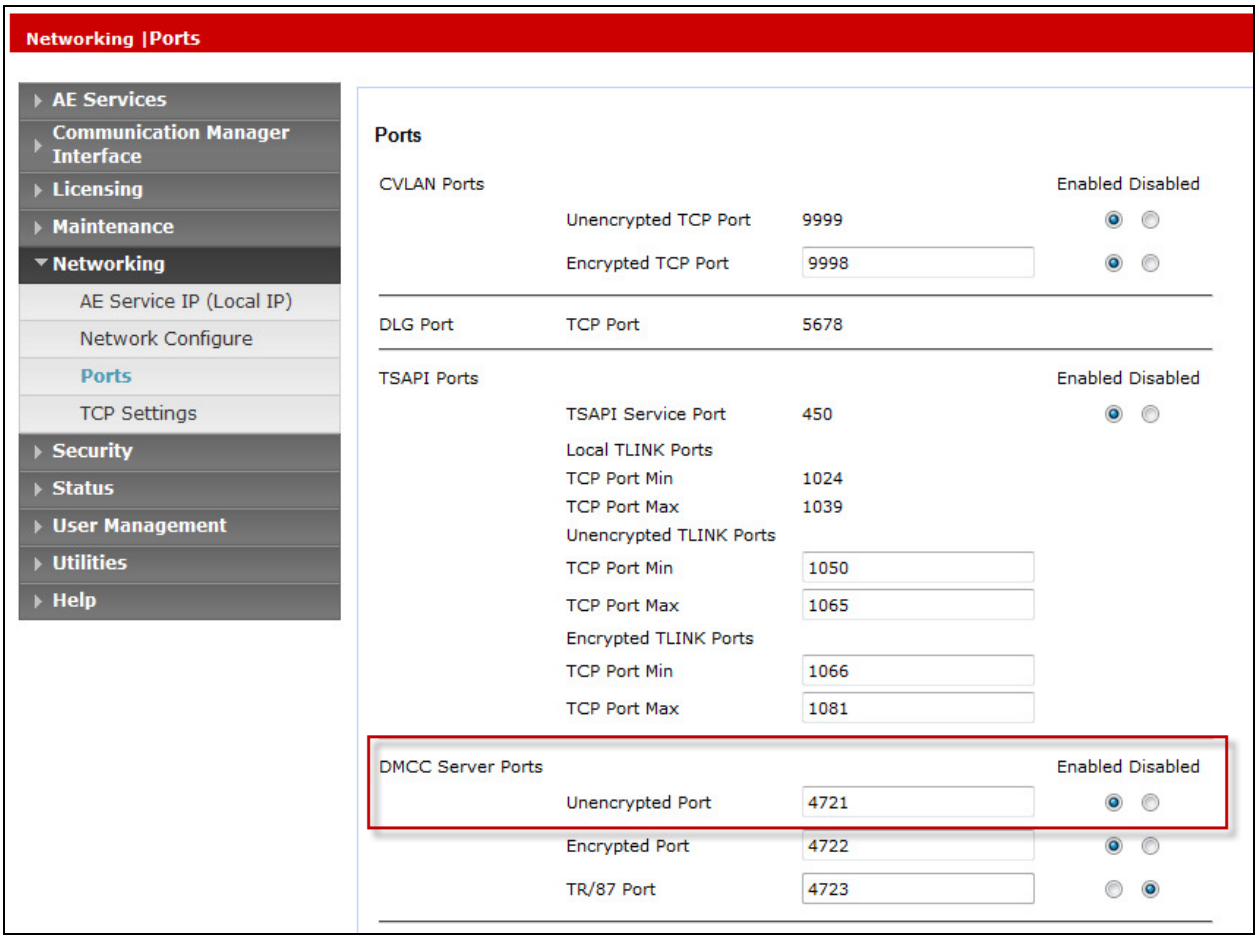
Navigate to the users screen by selecting **Security → Security Database → CTI Users → List All Users**. In the CTI Users window (not shown below), select the user that was set up in **Section 6.7** and select the Edit option.

In the **Edit CTI User** window assign access rights and call/device privileges according to customer requirements. For simplicity in configuration, **Unrestricted Access** was enabled during compliance testing. If Unrestricted Access is not desired, then consult **Reference [2]** for guidance on configuring the call/device privileges as well as devices and device groups. Click **Apply Changes**.



## 6.9. Administer DMCC Unencrypted Port

Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane. In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields. Click Apply Changes (not shown).



# 7. Configure OnviCord PRO

This section provides the procedure for configuring OnviCord PRO. The procedure includes the following areas:

- Installation of IMA Service
- Installation of IMS Service
- OnviCord PRO Device Configuration
    - Launch OnViews
    - Administer Devices For Recording

## 7.1. Installation of IMA Service

To configure the IMA Service for use with Application Enablement Services and Communication Manager, launch the IMA installer, **IMA_ServiceSetupAvaya.msi** provided by OnviSource. For brevity purposes, all steps are not shown. Please contact OnviSource for full installation instructions. The installer will guide you through the setup. Below is a description of the fields that will need to be populated during the setup.

**OnviCenter Database Location**: This is the IP of your **OnviCenter Data Server**. Note: can be **localhost** on a single box system.

**IMS Server IP**: This is the IP address of the recording server that you are installing the IMS on. Note: Must be in IP address format, DO NOT use localhost. This is the IP address that Avaya will stream audio to for recording.

**Group Name**: This is the group name you have predefined for this recording server and associated device.

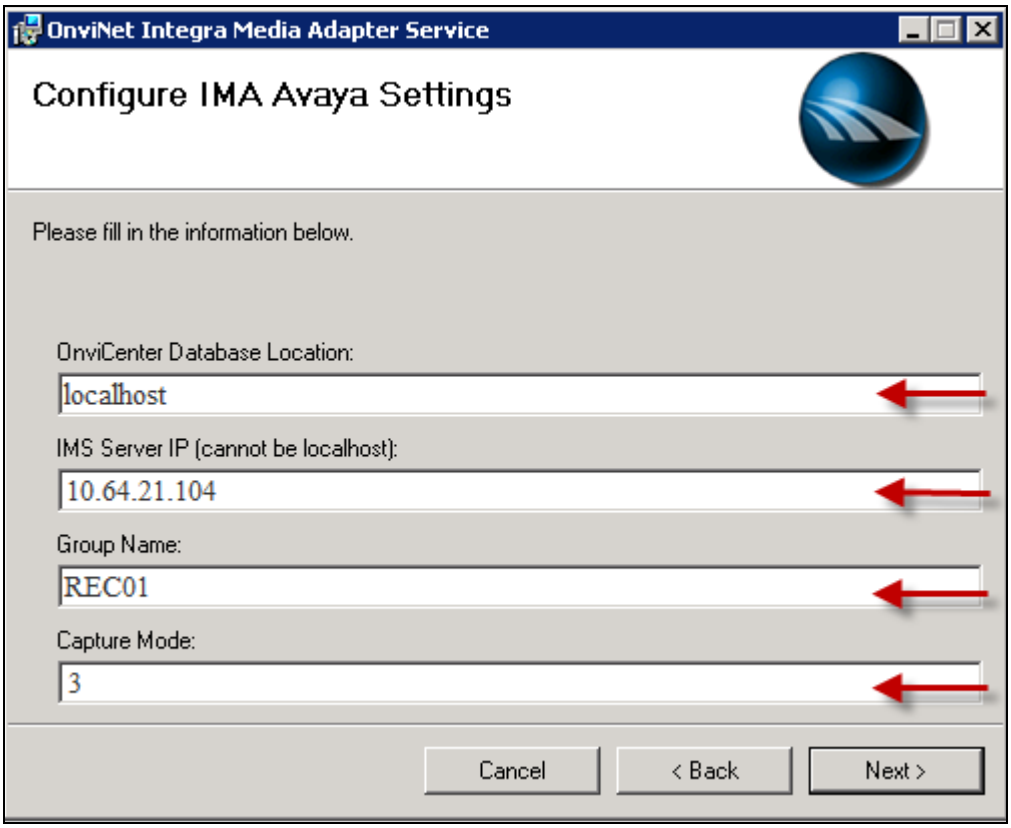
**Capture Mode**: Enter the capture Mode. Note: ONLY capture mode **3** is supported at this time.

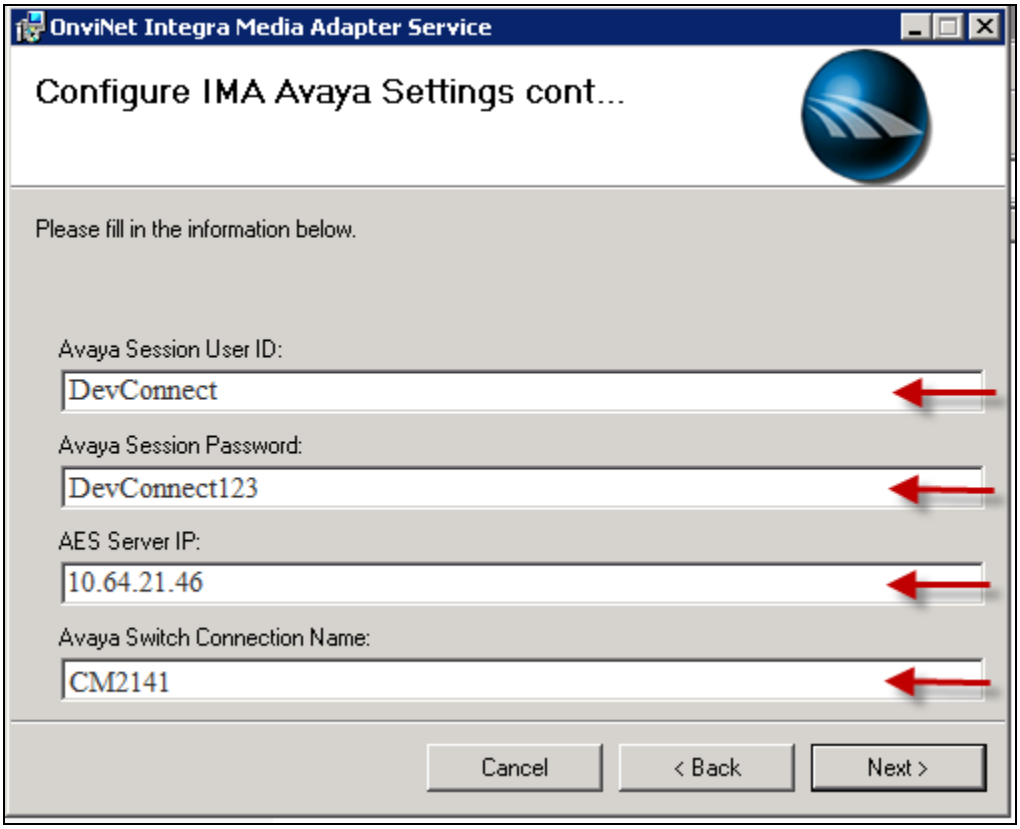
**Avaya Session User ID**: Enter the **User ID** administered in **Section 6.7**.

**Avaya Session Password**: Enter the **Password** administered in **Section 6.7**.

**Avaya AES IP**: Enter the IP address of the Application Enablement Services server.

**Avaya Switch Connection Name**: Enter in **Connection Name** administered in **Section 6.3**.



Output from the IMA_Services.exe file after the installation is complete.

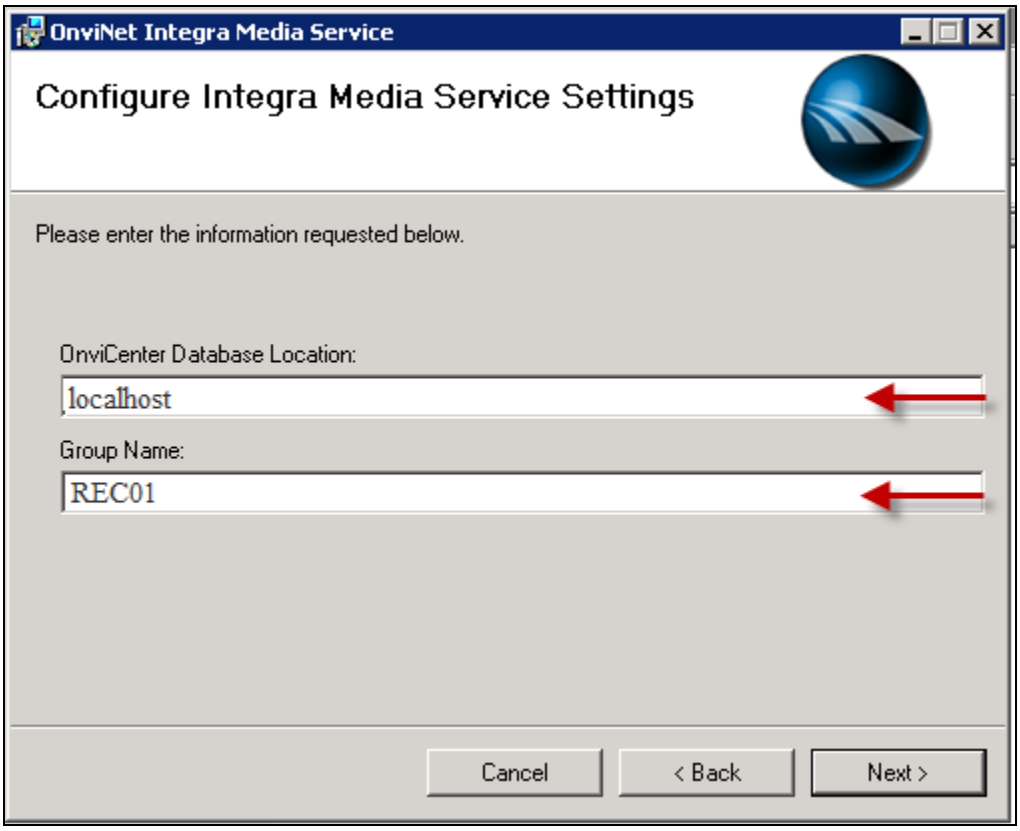
```
==================== My Settings ======================================== -->
   <add key="AvayaSessionUserName" value="DevConnect" />
   <add key="AvayaUserPassword" value="DevConnect123." />
   <add key="AvayaServiceProviderIP" value="10.64.21.46" />
   <add key="DataServerIP" value="localhost" />
   <!-- MediaIP:  Make sure this is set to the IP address of the machine     -->
   <!--    where the Media Service is installed.  Cannot be localhost.       -->
   <add key="MediaIP" value="10.64.21.104" />
   <add key="DefaultAvayaSwitchName" value="CM2141" />
   <add key="GroupName" value="REC01" />
   <!-- CaptureMode 0-None, 1-DisplayOnly, 2-MediaAndDisplay, 3-MediaOnly, 4-
SegmentRecordings-->
   <!-- Shown in OnViews:IntergraDeviceManager-->
   <add key="CaptureMode" value="3" />
   <add key="CtiLinkName" value="AVAYA#CM2141#CSTA#AES_21_46  " />
```

## 7.2. Installation of IMS Service

To configure the IMS Service for use with Application Enablement Services and Communication Manager, launch the IMS installer, **IntegraMediaServiceSetup.msi** provided by OnviSource. For brevity purposes, all steps are not shown. Please contact OnviSource for full installation instructions. The installer will guide you through the setup. Below is a description of the fields that will need to be populated during the setup.

**OnviCenter Database Location:** This is the IP of your **OnviCenter Data Server**. Note: can be localhost on a single box system.

**Group Name:** This is the group name you have predefined for this recording server and associated device. Note: This should be the same group name that was used when during the installation of the IMA service.




Output from the IntegraMediaService.exe file after the installation is complete

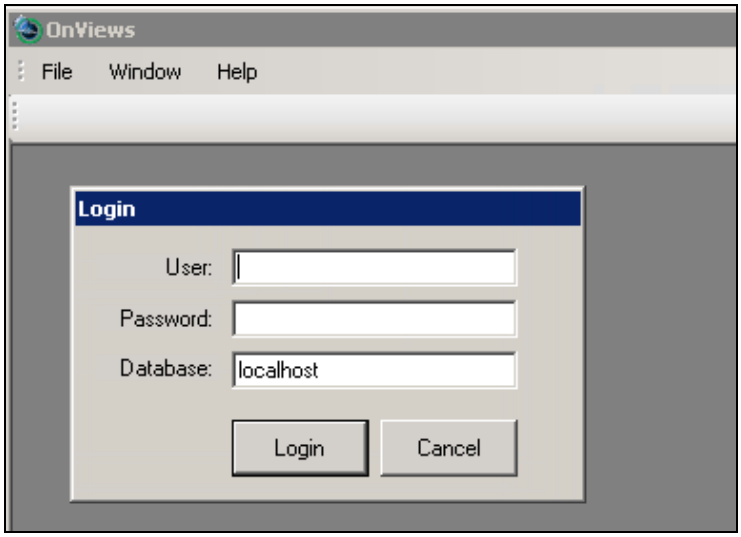

```
?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="DatabaseLocation" value="localhost" />
    <add key="DatabasePassword" value="zBuJDh42SHb5pr0mMtm5a81gM6TGZD1p" />
    <add key="OnviCordAgentVersion" value="13" />
    <add key="StopDelaySeconds" value="10" />
    <add key="EnableBuffering" value="true" />
    <add key="MinimumBufferSize" value="32768" />
    <add key="EnableRTPHandling" value="true" />
    <add key="GroupName" value="REC01"
                                                /
```

## 7.3. OnviCord PRO Device Configuration

The Integra Media Adapter (IMA) Manager provides access to data related to IMA service. The IMA Manger runs as a plug-in to OnViews.

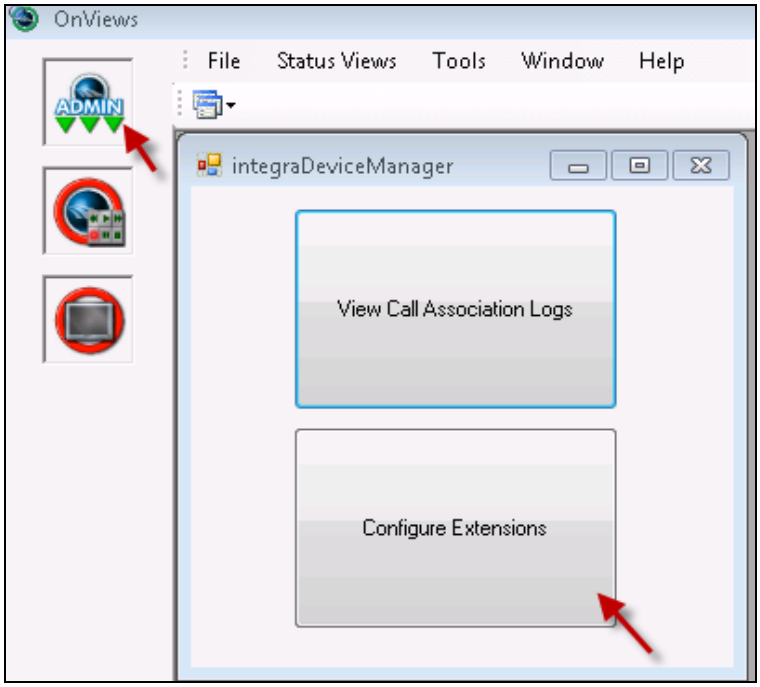
### 7.3.1. Launch OnViews

Launch OnViews by clicking the desktop icon. Log in by providing the appropriate **User** and **Password** credentials and entering localhost or the IP address of the OnviCenter DB in the **Database** field. Click **Login**.

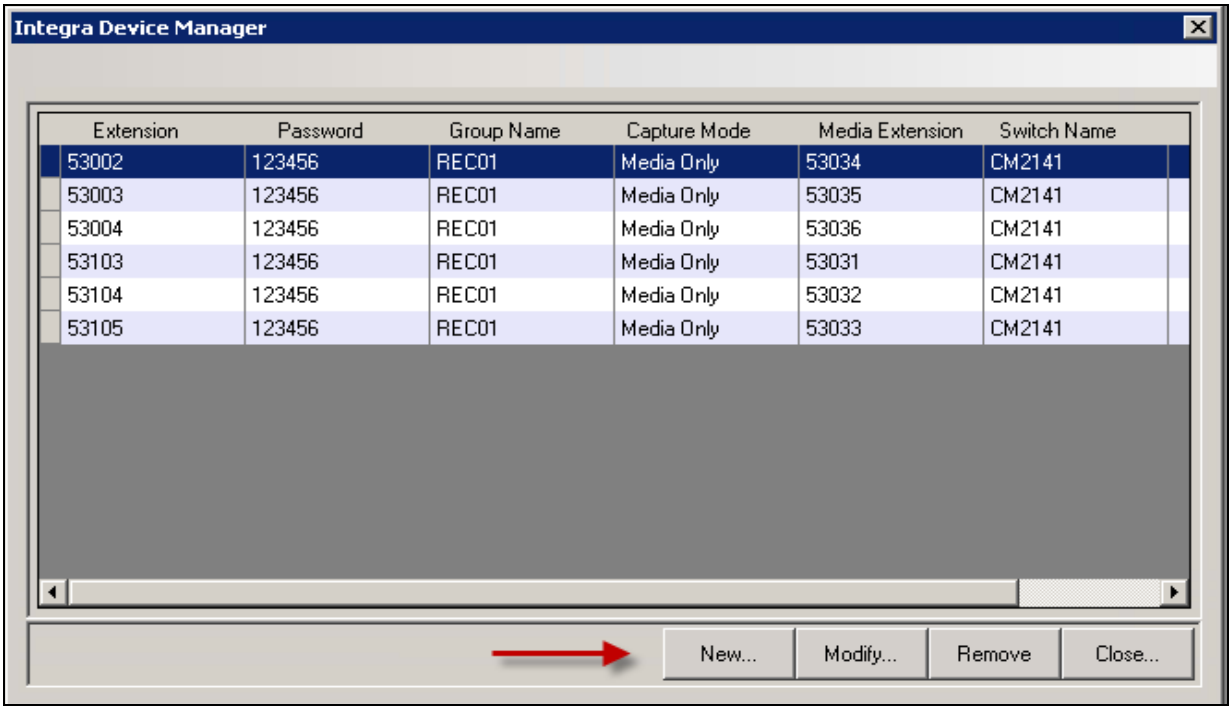


### 7.3.2. Administer Devices For Recording

To configure extensions on the **Integra Device Manager**, click on the **ADMIN** icon in the upper left corner. Click on **Configure Extensions**.




The Integra Device Manager dialog box, similar to the one below appears.



Each row in the table represents a single extension defined within the database that controls the behavior of the IMA/IMA service. To add a new extension, click the **New** button and provide the following information:

**Extension**: Enter the extension to be monitored. Make sure that the specified value matches an extension provisioned within the switch (i.e., Communication Manager). There is no harm in specifying an extension that isn't provisioned, but for the extension to be monitored, it must be fully configured within the switch.

**Password**: Enter the password associated with the station extension, as configured on Communication Manager.

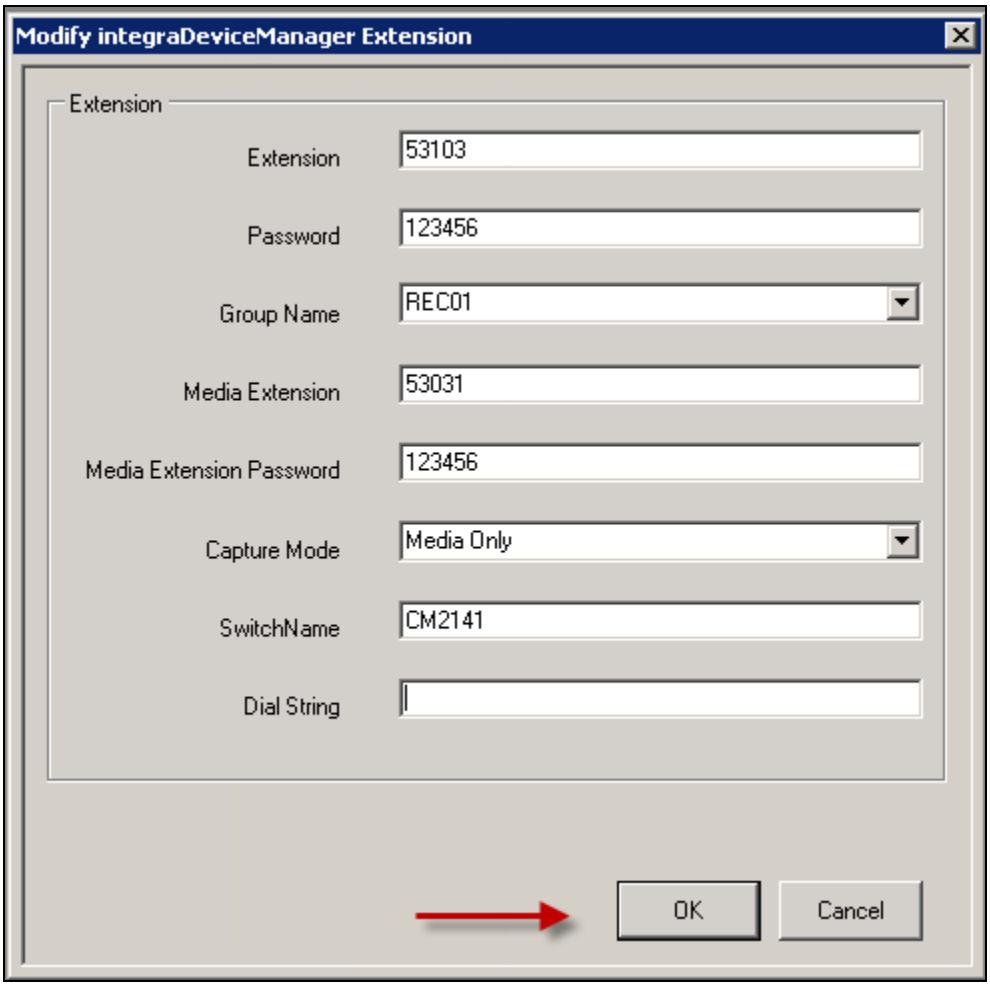
**Group Name**: This is an arbitrary descriptive label. It is used to associate the extension with a specific instance of the IMA/IMA service. Each instance of the IMA/IMA service has a unique group name (defined in its configuration file). A given instance of the service only monitors extensions having a group name equal to its own. This feature allows multiple instances of the service to run simultaneously without interfering with each other's extensions.

**Media Extension**: Enter the extension number of the DMCC recording device, administered in **Section 5.6**, used to capture audio media for calls to the primary extension.

**Media Extension Password**: Enter the password associated with the DMCC recording device, as configured on Communication Manager.

**Capture Mode**: Media Only mode is currently the only option supported for Capture Mode. This value should correspond to "**mode 3**" when installing IMA service from **Section 7.1**.

**Dial string**: Not currently supported, and should not be populated.




Click **Ok** to save changes.

# 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and OnviCord PRO.

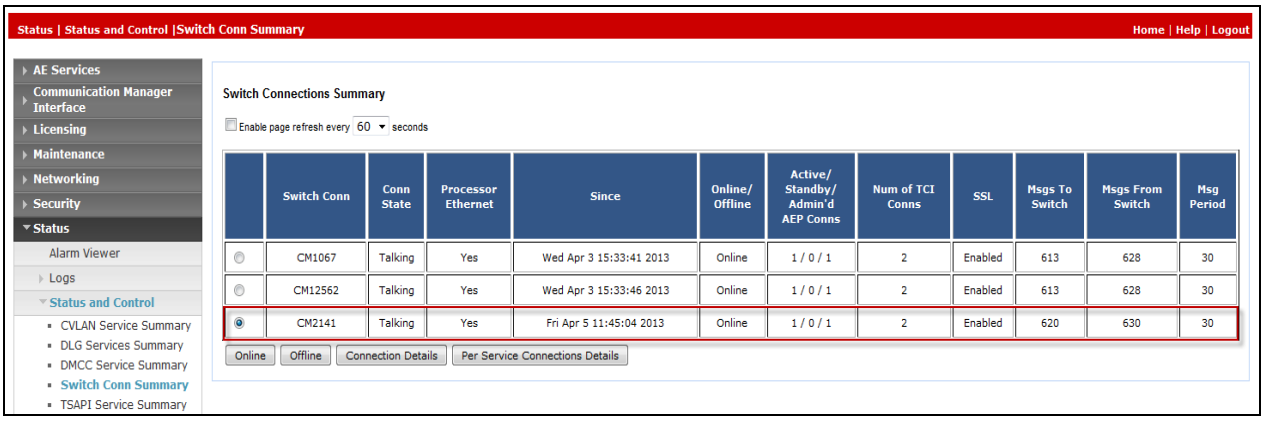
## 8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is **established** for the **CTI link** number administered in **Section 5.4**, as shown below.

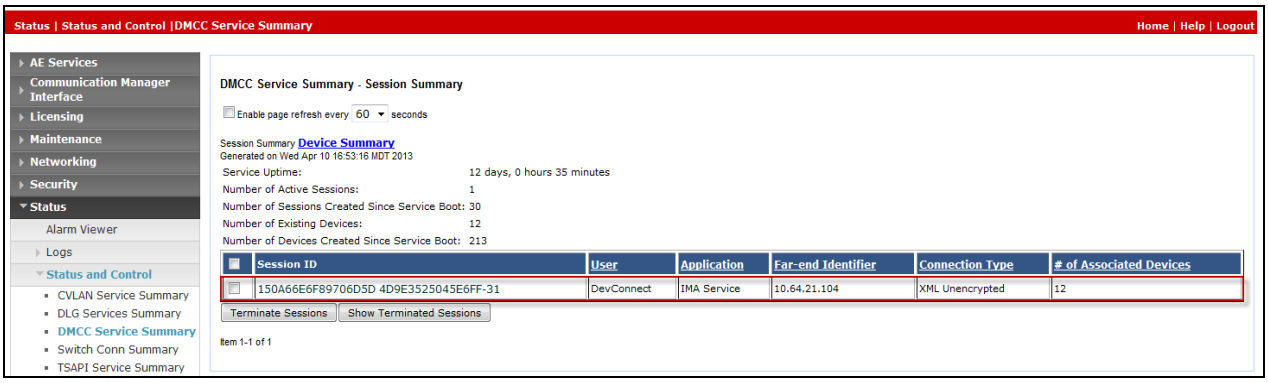
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1      4        no     AES_21_46        established    14        14
```

## 8.2. Verify Avaya Aura® Application Enablement Services

Verify the **Switch Connection** status by selecting **Status → Status and Control → Switch Case Summary** from the left pane. Verify **Conn State** is **Talking**.



Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. Verify that the **User** column shows an active session with the user name from **Section 6.7**, and that the **# of Associated Devices** column reflects the number of DMCC media extensions and endpoints being recorded.



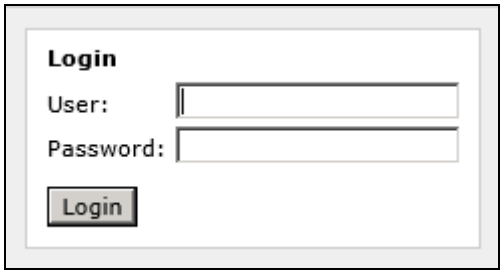

## 8.3. Verify Recordings

This section provides the steps required to verify calls are being properly recorded.

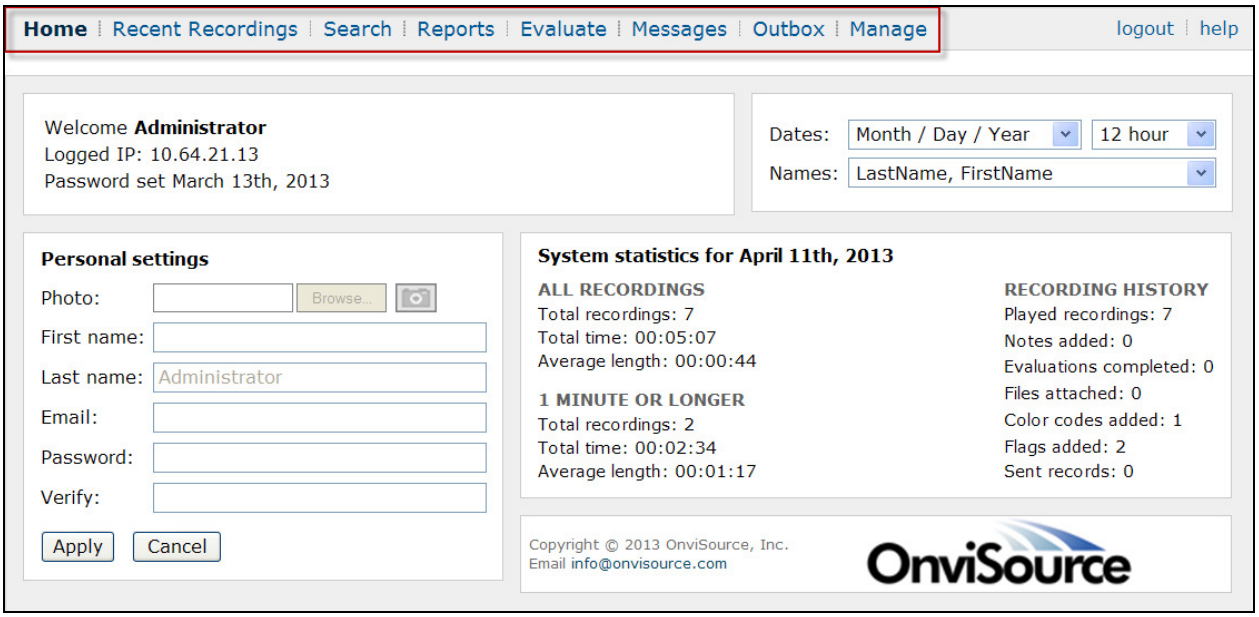
1. Place a few test calls to be recorded.

2. Log into "OnviCord Web". To log into "OnviCord Web" from the OnviCord Agent application residing on a PC running OnviCord Client, double click on the **OnviCord Web** icon residing on the desktop. To log into "OnviCord Web" from OnViews, click the **OnviCord Web** icon from the left menu bar (not shown).

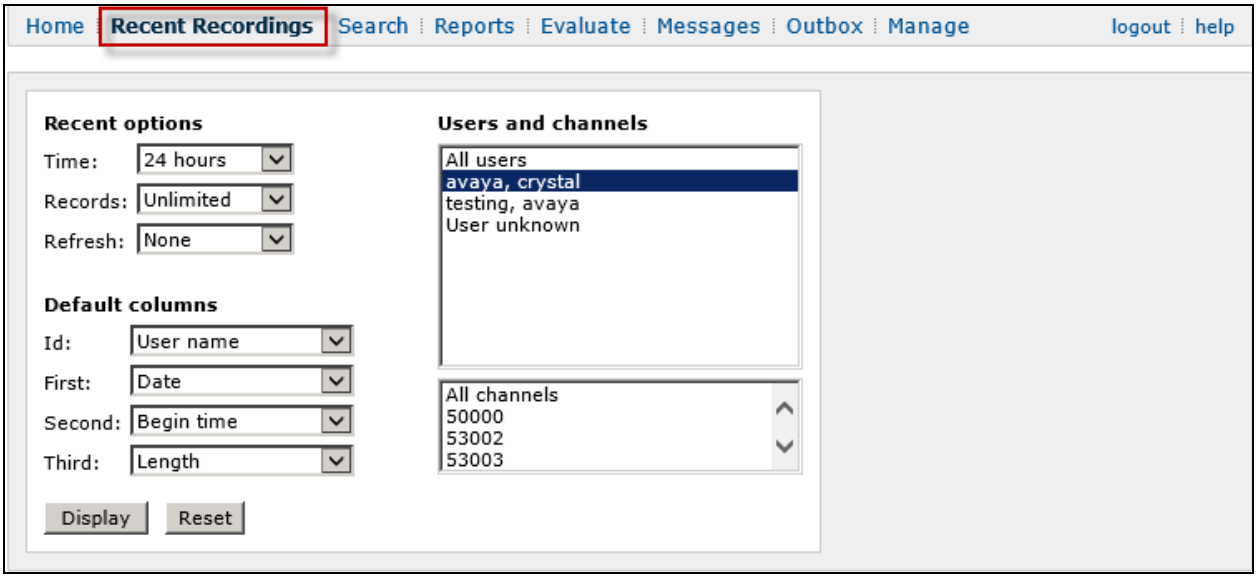
**Note**: Your OnviCord administrator determines which levels of "OnviCord Web" you may access. Depending on your privileges, you may not have access to all areas of "OnviCord Web".



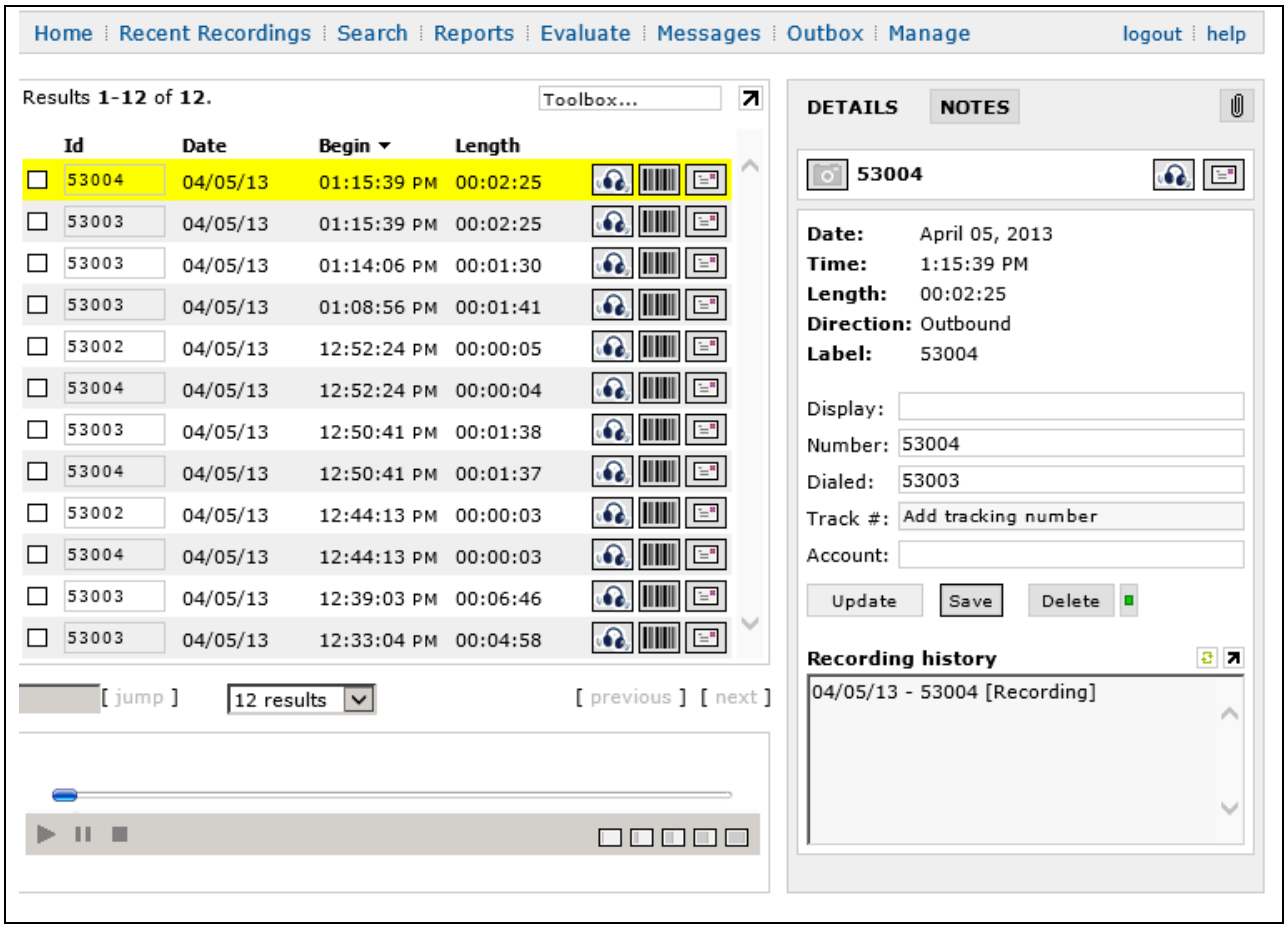
3. The "OnviCord Web" home window will be opened. Click **Recent Recordings** on the top of "OnviCord Web" screen to display a list of recent recordings.




4. Note, the first time you access Recent **Recordings**; you will be prompted to set preferences indicating what records to view and how they are displayed. In the **Recent options** section, use the drop-down box to view recent recordings within a specific time frame (a range between five minutes and one week) or a fixed of recent recordings (a range between 10 recordings to an unlimited maximum).



5. The results page shows a list of recordings on the left. Details about the first call on the page (which is highlighted) are shown on the right. Verify the details of the test calls are correct.




6. Click the headphones (or computer monitor) next to a recording to play the recording. For each test call, verify the quality of the recording and that the entire call was recorded.

# 9. Conclusion

These Application Notes describe the configuration steps required for OnviCord PRO 6.2 to successfully interoperate with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Application Enablement Services 6.2. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

# 10. Additional References

This section references the product documentation relevant to these Application Notes.

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


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

[2] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.2, Issue 1, July 2012.


OnviSource product documentation can be obtained by using the contact details in **Section 2.3**.


[3] *OnviSource OnviCord PRO, Installation and User's Manual*, 6.2.

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.