



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for OnviSource OnviCord with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services – Issue 1.1**

### **Abstract**

These Application Notes describe the configuration steps required for OnviSource OnviCord to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services.

OnviCord is a software-only solution for voice call recording that offers various recording, playback, and archiving features and options.

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

OnviSource OnviCord is a software-only solution for voice call recording that offers various recording, playback, and archiving features and options. 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 OnviSource server other than standard network connections.

OnviCord uses the Device Media and Call Control (DMCC) interface of Avaya Aura™ Application Enablement Services to monitor stations and obtain call events. OnviCord also uses the DMCC interface to register DMCC softphones with Communication Manger. The DMCC softphones are used as recording devices. When a call is to be record, OnviCord uses the Single Step Conferencing feature to bring a DMCC softphone into the call and to obtain the audio.

## 1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on feature functionality, serviceability, and performance. The feature functionality testing evaluated the ability of OnviSource OnviCord to monitor and record calls placed to and from stations on Communication Manager. The serviceability testing introduced failure conditions to see if OnviCord could properly resume recording calls after each failure recovery. The performance testing stressed OnviCord by continuously placing calls over extended periods of time.

The compliance testing validated the monitoring and recording performed by OnviCord of calls placed to and from analog phones, digital phones, IP phones, softphones, agents, Vector Directory Numbers (VDNs), and hunt groups on an Avaya Media Server running Communication Manager.

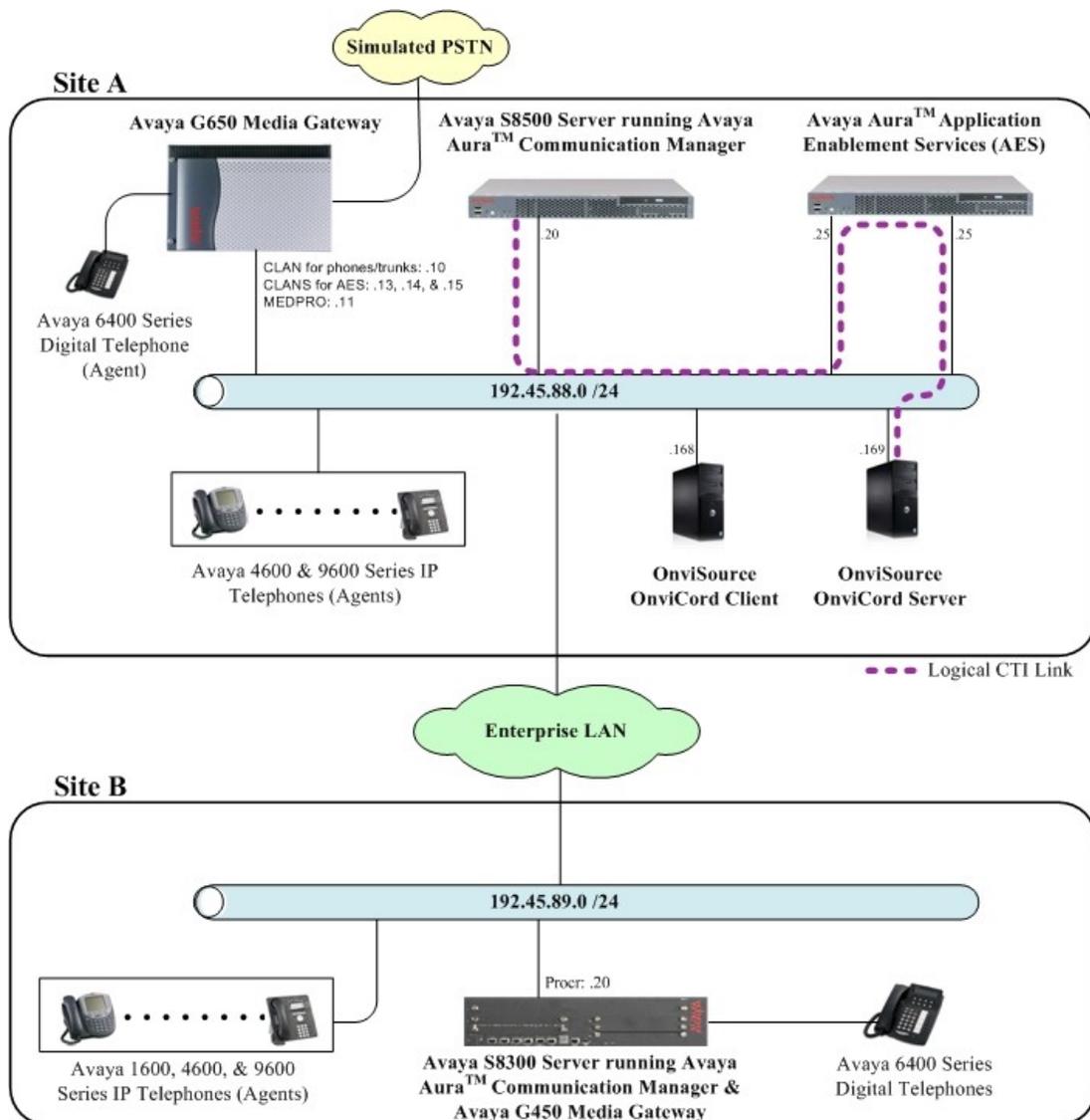
## 1.2. Support

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

- Phone: 1-800-388-8402
- Web: <http://www.onvisource.com/support/index.php>
- Email: [support@onvisource.com](mailto:support@onvisource.com)

## 2. Reference Configuration

The figure below shows the configuration used during compliance testing. Site A is comprised of an Avaya S8500 Media Server with an Avaya G650 Media Gateway. Site B is comprised of an Avaya S8300 Media Server with an Avaya G450 Media Gateway. At each site, Communication Manager runs on the Avaya Media Server. The two Communication Manager systems are connected to each other via an IP (H.323) trunk and an ISDN-PRI trunk. The various telephones shown are used to generate intra-switch calls (calls between telephones on the same system), outbound/inbound calls to/from the PSTN, and inter-switch calls (calls between the two Communication Manager systems via the two trunks). The OnviSource OnviCord server is set up to record calls at Site A.



**Figure 1: OnviSource OnviCord with Communication Manager and AES**

### 3. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server (w/ G650)	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya S8300 Server (w/ G450)	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya G650 Media Gateway: TN799DP (C-LAN) TN2602AP (MEDPRO) TN2312BP (IPSI)	HW01, FW026 HW02, FW007 HW15, FW030
Avaya G450 Media Gateway : MM710BP (DS1) MM712AP (DCP)	HW11, FW044 HW07, FW009
Avaya Aura™ Application Enablement Services (AES) Server	4.2
Avaya 1600 Series IP Phones : 1608SW (H.323) 1616SW (H.323)	1.0.3 1.0.3
Avaya 4600 Series IP Phones: 4610SW (H.323) 4620SW (H.323) 4621SW (H.323)	2.9 2.9 2.9
Avaya 9600 Series IP Phones: 9620 (H.323) 9630 (SIP)	3.002 2.4.1
Avaya 6400 Series Digital Phones	-
OnviSource OnviCord Server	6.1.3
OnviSource OnviCord Client	6.1.3

## 4. Configure 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]**.

The information shown on the screens throughout this section indicate the values that were used during compliance testing.

### 4.1. Configure IP Codec Sets & IP-Network Regions

This section provides the steps required for configuring an ip-codec-set and ip-network regions.

1. Enter the **change ip-codec-set <codec set number>** command, where **<codec set number>** is the codec set number to be used with the OnviSource recording solution.
  - In the **Audio Codec** field, type **G.711MU**.

```
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
2:
3:
```

2. Enter the **change ip-network-region <region number>**, where **<region number>** is the ip network region number to be used with the OnviSource recording solution.
  - In the **Code Set** field, enter the **<codec set number>** administered in **Step 1**. The **Codec Set** field reflects the codec set that must be used for connections between phones within this region or between phones and the media processor boards in the Avaya Media Gateway within this region.

```

change ip-network-region 1                                     Page 1 of 19
                                                              IP NETWORK REGION
Region: 1
Location: 1          Authoritative Domain: dev8.com
Name: interop
MEDIA PARAMETERS
  Codec Set: 1          Intra-region IP-IP Direct Audio: yes
                      Inter-region IP-IP Direct Audio: yes
                      IP Audio Hairpinning? y
  UDP Port Min: 2048
  UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 48      RTCP Reporting Enabled? y
  Audio PHB Value: 48            RTCP MONITOR SERVER PARAMETERS
  Video PHB Value: 26           Use Default Server Parameters? y
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5
H.323 IP ENDPOINTS
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
                                                              AUDIO RESOURCE RESERVATION PARAMETERS
                                                              RSVP Enabled? n

```

During compliance testing, two IP Network regions were used. It is best practice for all CLANs dedicated to Application Enablement Services to be in a separate network region from those CLANs servicing endpoints (i.e. phones). For compliance testing, a single CLAN in network region 1 was used to service endpoints, while 3 CLANs in network region 2 were dedicated to Application Enablement Services. Both IP network regions were configured to use IP codec set 1.

## 4.2. Configure Connectivity to Application Enablement Services and Endpoints

This section provides the steps required for configuring connectivity from Communication Manager to Application Enablement Services and endpoints.

The Application Enablement Services server communicates with Communication Manager by using one or more CLANs to create a switch connection. The following steps show only the configuration required in Communication Manager to set up a switch connection. See **Section 5.1** for the configuration steps required in Application Enablement Services to complete the administration of the switch connection.

1. Enter the **change node-names ip** command.

- In the **Name** field, type a descriptive name to assign to a CLAN to be administered.
- In the **IP Address** field, type the IP address assigned to the CLAN.

```
change node-names ip                                     Page 1 of 2
IP NODE NAMES
Name            IP Address
8300            192.45.89.20
CLAN            192.45.88.10
CLAN2          192.45.88.13
CLAN3          192.45.88.14
CLAN4          192.45.88.15
LSP-8300       192.45.88.30
Member-CDR     192.168.199.69
RDTT-CDR       192.45.88.45
SES            192.45.88.50
cf-medpro      192.45.88.11
default        0.0.0.0
ipoffice       192.45.88.40
procr          192.45.88.20
```

Repeat this step for each CLAN.

In the compliance tested configuration, the **CLAN** node was used for registering endpoints and the **CLAN2**, **CLAN3**, and **CLAN4** nodes were used for connectivity to Application Enablement Services.

2. Enter the **add ip-interface <board location>** command, where **<board location>** is the board location for the CLAN, for example: 01A02.

- In the **Enable Interface** field, type **y**.
- In the **Network Region** field, type the network region number administered in **Section 4.1**.
- In the **Node Name** field, enter the **Name** from **Step 1**.
- In the **Ethernet Link** field, type an available Ethernet link number.

```

add ip-interface 01a02                                     Page 1 of 3
                                                           IP INTERFACES
                                                           Type: C-LAN
                                                           Slot: 01A02           Target socket load and Warning level: 400
                                                           Code/Suffix: TN799 D   Receive Buffer TCP Window Size: 8320
Enable Interface? y                                     Allow H.323 Endpoints? y
                                                           VLAN: n               Allow H.248 Gateways? y
Network Region: 1                                     Gatekeeper Priority: 5

                                                           IPV4 PARAMETERS
                                                           Node Name: CLAN
                                                           Subnet Mask: /24
                                                           Gateway Node Name:

Ethernet Link: 1

```

Repeat this step for each CLAN

In the compliance tested configuration, the **CLAN** node was assigned to network region 1 and the **CLAN2**, **CLAN3**, and **CLAN4** nodes were assigned to network region 2.

3. Enter the **change ip-services** command.

- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type **<nodename>**, where **<nodename>** is the name of the CLAN board used for connectivity to Application Enablement Services.
- In the **Local Port** field, accept the default port (**8765**).

```

change ip-services                                         Page 1 of 4
                                                           IP SERVICES
Service Type      Enabled   Local Node      Local Port      Remote Node      Remote Port
AESVCS            y        CLAN2           8765
AESVCS            y        CLAN3           8765
AESVCS            y        CLAN4           8765

```

Repeat this step for each CLAN used for connectivity to Application Enablement Services.  
On **Page 4**,

- In the **AE Services Server** field, type the <name> of the Application Enablement Services server. On the Application Enablement Services server, the name can be obtained by typing “uname -n” at the command prompt. The name entered on Communication Manager must match the Application Enablement Services server name exactly.
- In the **Password** field, enter an alphanumeric password. The passwords must exactly match on both Communication Manager and the Application Enablement Services (administered in **Section 5.1**).
- In the **Enabled** field, type **y**.

```
change ip-services
```

Page 4 of 4

AE Services Administration

Server ID	AE Services Server	Password	Enabled	Status
1:	aeserver25	xxxxxxxxxxxxxx	y	in use
2:				
3:				

### 4.3. Configure CTI Link

This section provides the steps required for configuring a CTI link on Communication Manager. See **Section 5.3** for the configuration steps required on Application Enablement Services to complete the administration.

1. Enter the **display system-parameters customer-options** command.

- On **Page 3**, verify that the **Computer Telephony Adjunct Links** field is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.

```
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? n   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? n
ARS/AAR Dialing without FAC? y           DCS (Basic)? y
ASAI Link Core Capabilities? y           DCS Call Coverage? y
ASAI Link Plus Capabilities? y           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
```

2. Enter **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
add cti-link 10                                                         Page 1 of 3
                                CTI LINK
CTI Link: 10
Extension: 39010
Type: ADJ-IP
Name: TSAPI Link 1 - aeserver25
                                COR: 1
```

## 4.4. Configure Stations (DMCC Recording Devices)

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

For the purpose of this document, devices that have been registered using the DMCC service will be called “DMCC devices”. When a client application registers itself as a DMCC device at an extension, it can act like an IP softphone to control and monitor physical aspects of the extension (button pushes, lamps, the display, etc.) or access and control the media streams at the extension. For a client application to be able to control the media at an extension, and record calls at that extension, it must register itself as a DMCC device with the media mode set to “Client”. Client media mode indicates that the client application will handle the media streams from the DMCC device. DMCC devices that have been registered in Client media mode will be called “DMCC recording devices”.

The DMCC recording devices used by OnviSource OnviCord are administered as IP softphones on Avaya Communication Manager. Each DMCC recording device requires either an “IP\_API\_A” license on Communication Manager or a “VALUE\_DMCC\_DMC” license on Application Enablement Services.

Note that these licenses are separate and independent from the Avaya IP Softphone licenses that are required on Communication Manager for Avaya IP Softphones, but not for DMCC recording devices.

1. Enter the **display system-parameters customer-options** command to verify that there are sufficient **IP\_API\_A** licenses for the DMCC recording devices. If not, contact an authorized Avaya account representative to obtain these licenses.

```
display system-parameters customer-options Page 10 of 11
MAXIMUM IP REGISTRATIONS BY PRODUCT ID
```

Product ID	Rel. Limit	Used
<b>IP_API_A</b>	<b>: 1000</b>	<b>0</b>
IP_API_B	: 1000	0
IP_API_C	: 1000	0
IP_Agent	: 1000	0
IP_IR_A	: 0	0
IP_Phone	: 2400	3
IP_ROMax	: 2400	0
IP_Soft	: 2	0
IP_eCons	: 0	0
oneX_Comm	: 2400	0
	: 0	0

2. Enter the **add station <extension>** command, where **<extension>** is a valid station extension.
  - In the **Type** field, type an IP telephone set type with configurable buttons; for example, **4620**.
  - In the **Security Code**, type the value entered for **<extension>** (the station extension and security code must match).
  - In the **Name** field, type a descriptive name.
  - In the **IP SoftPhone**, type **y**.

```

add station 31126                                     Page 1 of 5
                                                    STATION
Extension: 31126                                     Lock Messages? n          BCC: 0
  Type: 4620                                         Security Code: 31126      TN: 1
  Port: IP                                           Coverage Path 1:         COR: 1
  Name: DMCC Softphone                               Coverage Path 2:         COS: 1
                                                    Hunt-to Station:
STATION OPTIONS
  Loss Group: 19                                     Time of Day Lock Table:
  Speakerphone: 2-way                               Personalized Ringing Pattern: 1
  Display Language: english                         Message Lamp Ext: 31126
  Survivable GK Node Name:                          Mute Button Enabled? y
  Survivable COR: internal                           Expansion Module? n
  Survivable Trunk Dest? y                           Media Complex Ext:
                                                    IP SoftPhone? y
                                                    IP Video? n
                                                    Customizable Labels? Y

```

Repeat **Step 2** for each DMCC recording device required for the configuration. During compliance testing, 23 DMCC recording devices were administered to be able to record up to 23 calls simultaneously.

This completes the Communication Manager configuration.

## 5. Configure Application Enablement Services

The Application Enablement Services (AES) server 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 assumes that the installation and basic administration of the Application Enablement Services server has already been performed. For more information on administering Application Enablement Services, refer to the Avaya product documentation, **Reference [2]**.

1. Launch a web browser and enter <https://<IP address of AES Server>> in the address field. Click **AE Server Administration**.



[AE Server Administration](#)  
[WebLM Administration](#)

Welcome to Avaya Application Enablement Services

These web pages are provided for the administration and maintenance of this Avaya Application Enablement Server.

Before You Begin:

\*\*\* WARNING NOTICE \*\*\*

This system is restricted solely to Avaya authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited by Avaya. Unauthorized users are subject to Company disciplinary proceedings and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if monitoring reveals possible evidence of criminal activity, Avaya may provide the evidence of such activity to law enforcement officials. All users must comply with Avaya Security Instructions regarding the protection of Avaya's information assets.

© 2007 Avaya Inc. All Rights Reserved.

2. Log in with the appropriate credentials for accessing the Application Enablement Services CTI OAM web pages.



- Click **CTI OAM Administration** in the left pane menu.

**AVAYA** Application Enablement Services  
Operations Administration and Maintenance

You are here: > Home

**Welcome to OAM**

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

- CTI OAM Admin - Use CTI OAM Admin to manage all AE Services that you are licensed to use on the AE Server.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Security Administration - Use Security Administration to manage Linux user accounts and configure Linux-PAM (Pluggable Authentication Modules for Linux).

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

- Verify that Application Enablement Services is licensed for the TSAPI and DMCC services. If these services are not licensed, contact an authorized Avaya account representative to obtain these licenses.

**AVAYA** Application Enablement Services  
Operations Administration and Maintenance

You are here: > CTI OAM Home

**Welcome to CTI OAM Screens**

[craft] Last login: Fri Mar 13 11:28:08 2009 from 192.45.88.45

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	Licenses Purchased
ASAI Link Manager	Running	N/A	N/A
<b>DMCC Service</b>	Running	ONLINE	Yes
CVLAN Service	Running	ONLINE	Yes
DLG Service	Running	ONLINE	Yes
Transport Layer Service	Running	N/A	N/A
<b>TSAPI Service</b>	Running	ONLINE	Yes
SMS	N/A	N/A	Yes

For status on actual services, please use [Status and Control](#).

**License Information**

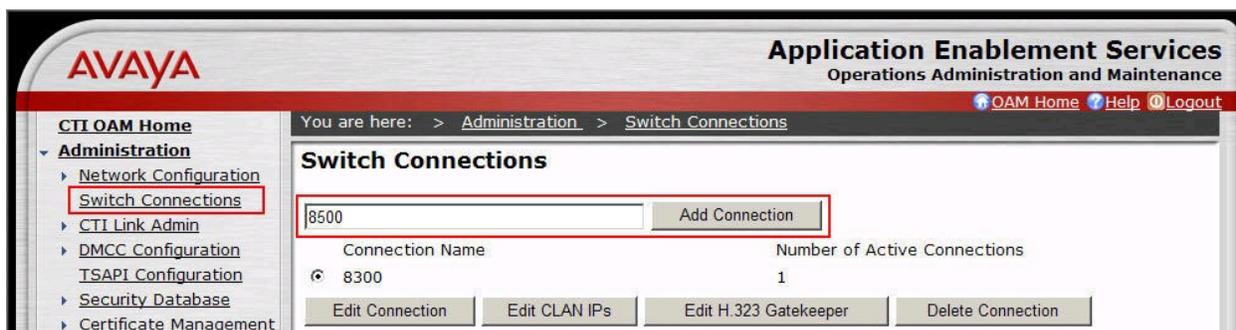
You are licensed to run Application Enablement (CTI) version 4.

- Each DMCC recording device used by OnviSource OnviCord requires either an “IP\_API\_A” license on Avaya Communication Manager or a “VALUE\_DMCC\_DMC” license on Application Enablement Services. If “VALUE\_DMCC\_DMC” licenses are being used, log in to the Avaya Web License Manager (WebLM) and verify that there are sufficient licenses for the DMCC recording devices. Additionally, verify there are sufficient TSAPI licenses. If not, contact an authorized Avaya account representative to obtain these licenses.

## 5.1. Configure a Switch Connection

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

- Select **Administration > Switch Connections** from the left pane menu. In the **Add Connection** field, type a descriptive name and click **Add Connection**.

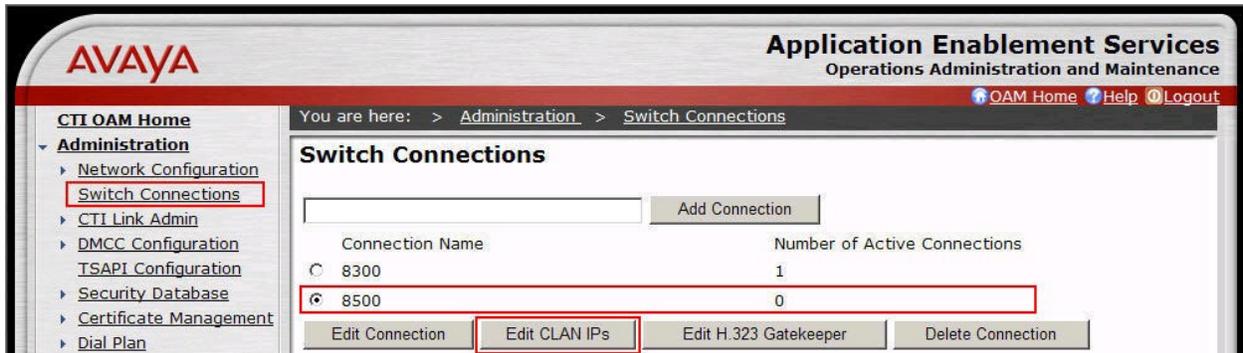


- In the **Switch Password** field, type the password that was entered during **Step 3** of **Section 4.2**. Re-type the password in the **Confirm Switch Password** field. Leave **SSL** checked if using a secure connection to Communication Manager. Click **Apply**.

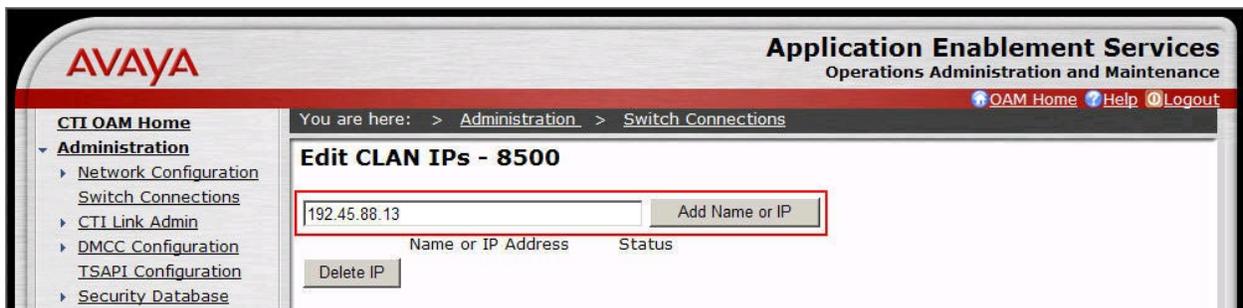


OAM adds the switch connection and returns to the “Switch Connections” page.

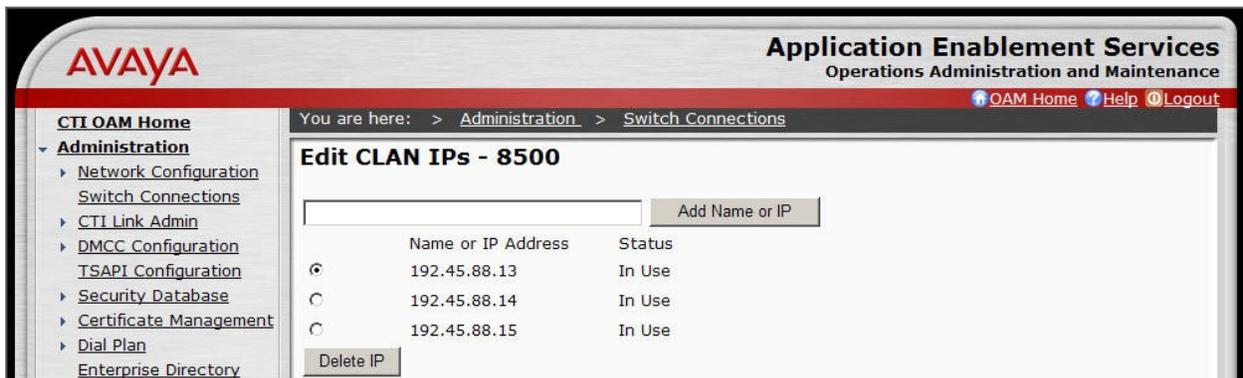
- From the “Switch Connections” page, select the newly added switch connection, and click **Edit CLAN IPs**.



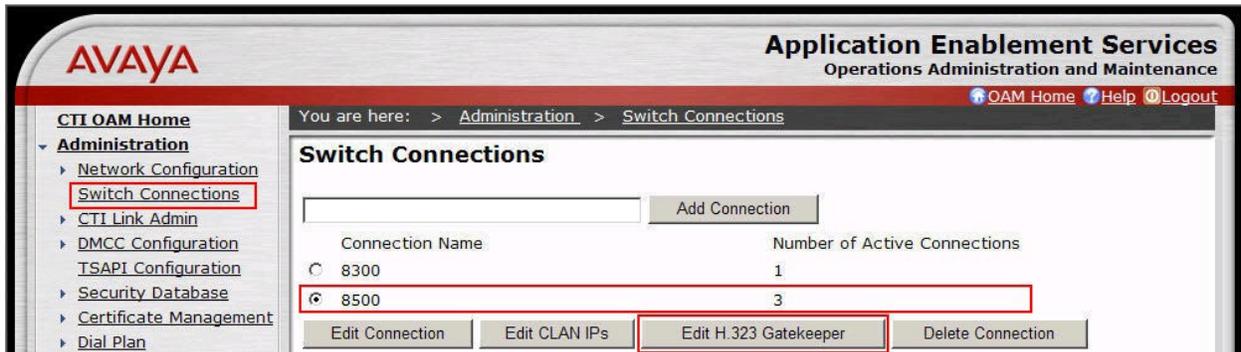
- In the **Add Name or IP** field, type the <Host Name> or the <IP Address> of the CLAN, and click **Add Name or IP** (use the Host Name or IP address of the CLAN that was administered for Application Enablement Services connectivity in **Section 4.2**).



Repeat this step for each CLAN. The screen below shows the CLANs that were used during compliance testing.



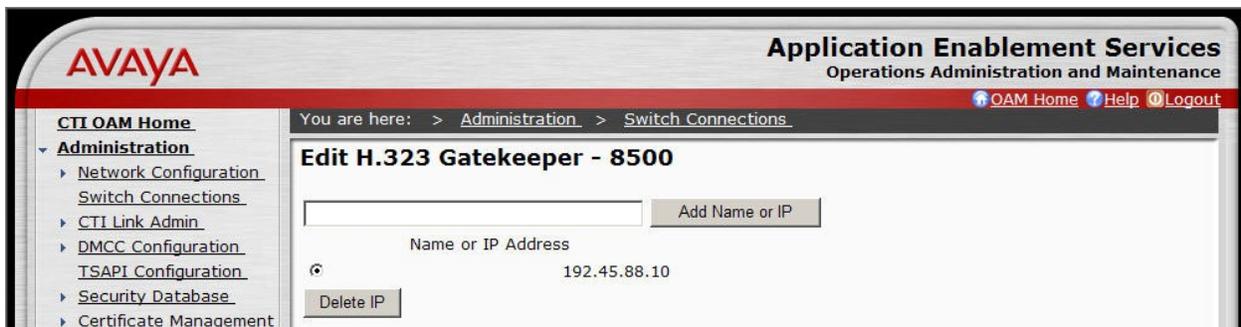
5. Navigate back to **Administration > Switch Connections**. Select the switch connection, and click **Edit H.323 Gatekeeper**.



6. In the **Add Name or IP** field, type the <Host Name> or <IP address> of the CLAN to be used for registering endpoints. Click **Add Name or IP**.



Repeat this step as necessary to add multiple H.323 Gatekeepers. The screen below shows the CLANs that were used during compliance testing.



## 5.2. Configure DMCC Server Ports

This section provides the steps required for configuring DMCC server ports.

1. Navigate to the **CTI OAM Home > Administration > Ports** page. During compliance testing, the default port values shown in the screen below were utilized. Since the unencrypted port was utilized during the compliance test, set the **Unencrypted Port** field to **Enabled**. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

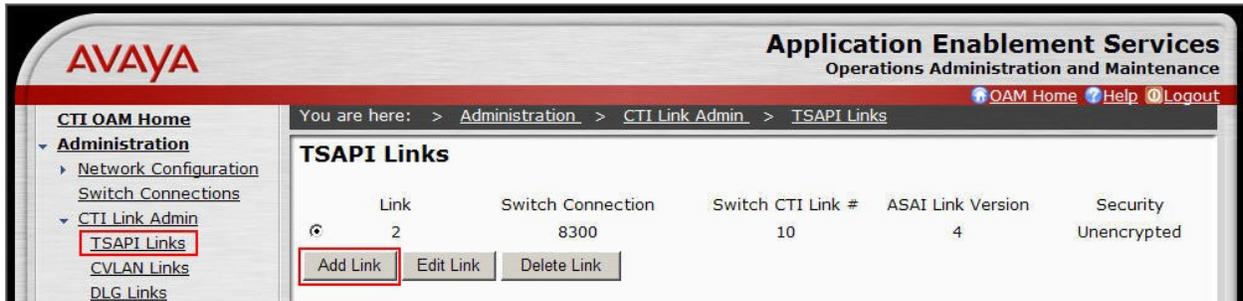
The screenshot shows the Avaya Application Enablement Services (AES) web interface. The page title is "Application Enablement Services" with the subtitle "Operations Administration and Maintenance". The breadcrumb trail is "You are here: > Administration > Network Configuration > Ports". The left sidebar contains a navigation menu with "Ports" highlighted in red. The main content area is titled "Ports" and is divided into several sections:

- CVLAN Ports:** A table with two rows: "Unencrypted TCP Port" (value 9999) and "Encrypted TCP Port" (value 9998). Each row has radio buttons for "Enabled" and "Disabled".
- DLG Port:** A single row: "TCP Port" (value 5678).
- TSAPI Ports:** A section with "Enabled Disabled" radio buttons. It includes:
  - TSAPI Service Port (value 450)
  - Local TLINK Ports:
    - TCP Port Min (value 1024)
    - TCP Port Max (value 1039)
  - Unencrypted TLINK Ports:
    - TCP Port Min (value 1050)
    - TCP Port Max (value 1065)
  - Encrypted TLINK Ports:
    - TCP Port Min (value 1066)
    - TCP Port Max (value 1081)
- DMCC Server Ports:** A section with "Enabled Disabled" radio buttons. It includes:
  - Unencrypted Port (value 4721) - This row is highlighted with a red border, and the "Enabled" radio button is selected.
  - Encrypted Port (value 4722)
  - TR/87 Port (value 4723)

### 5.3. Configure TSAPI Link

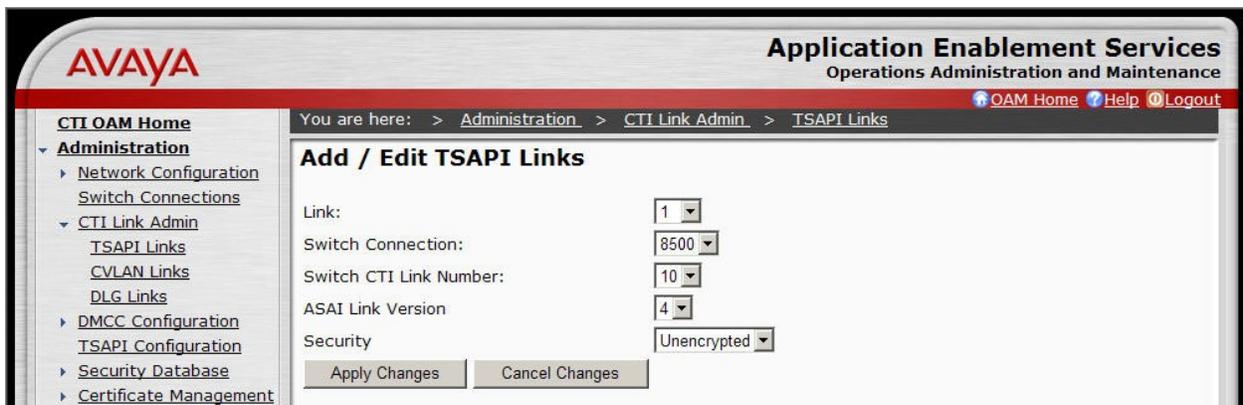
This section provides the steps required for configuring a TSAPI Link.

1. From the CTI OAM main menu select **Administration > CTI Link Admin > TSAPI Links**. Click **Add Link**.



2. Complete the “Add / Edit TSAPI Links” page as follows:

- In the **Link** field, select an available link number.
- In the **Switch Connection** field, select the switch connection configured in **Section 5.1**.
- In the **Switch CTI Link Number** field, select the CTI link number that was administered on Communication Manager in **Step 2 of Section 4.3**.
- In the **ASAI Link Version** field, select the default value, **4**.
- In the **Security** field, select the appropriate encryption option for connectivity to the OnviSource OnviCord server.

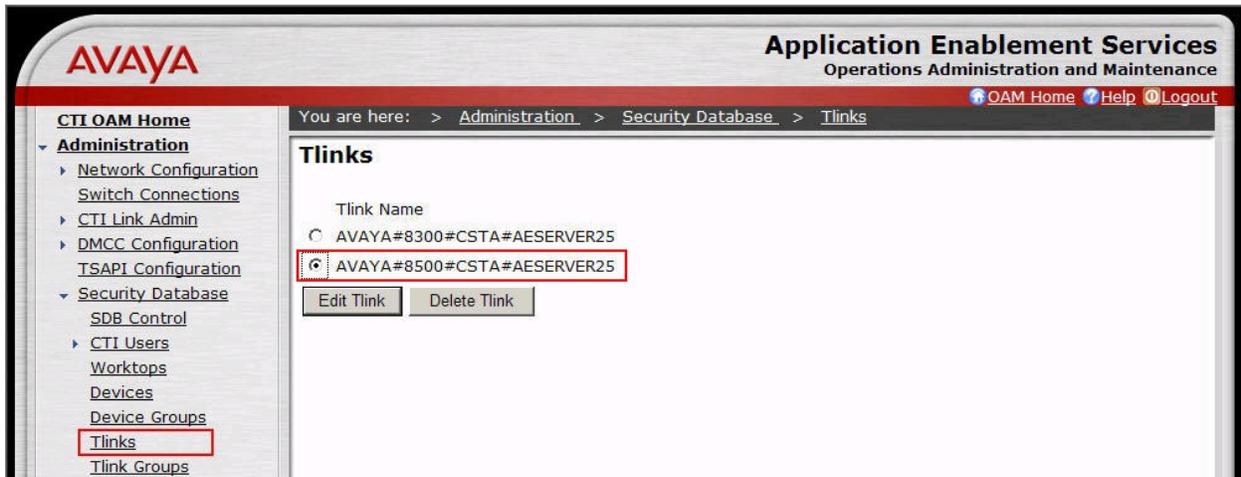


## 5.4. Display Tlink

This section provides the steps required to display Tlinks.

Tlinks are service identifiers (names) dynamically created by the TSAPI Service. Tlinks are created automatically once the TSAPI CTI links are created. The appropriate Tlink name will be needed during the configuration of the OnviSource OnviCord server. This section just illustrates how to obtain the Tlink name.

1. Navigate to **Administration > Security Database > CTI Users > Tlinks**.



To identify the correct Tlink, note that a Tlink has the following format:

**AVAYA#switch\_connection\_name#service\_type#AE\_server\_name**

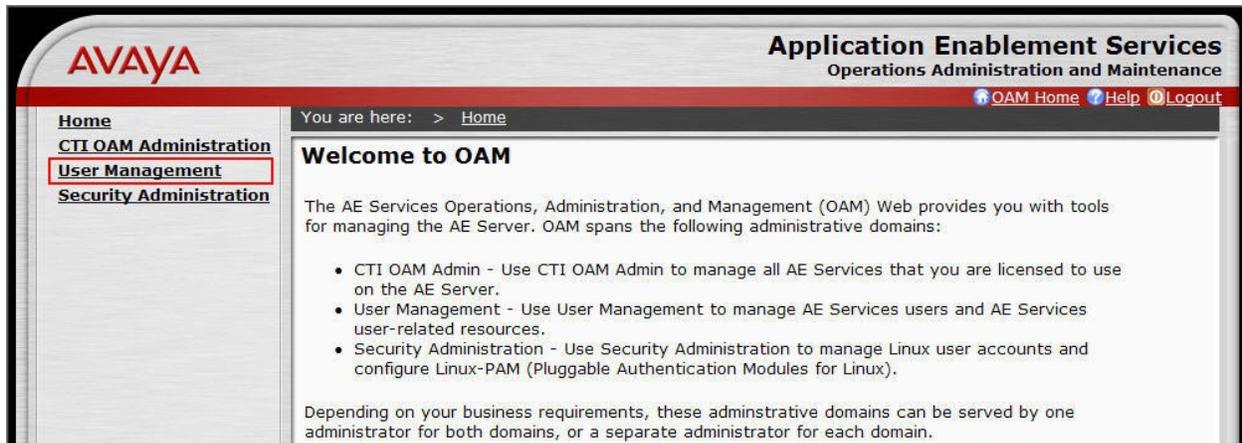
where:

- **AVAYA** is a fixed constant.
- **switch\_connection\_name** represents the Switch Connection name administered in **Section 5.1**.
- **service\_type** refers to the CSTA service type. It can be either of the following:
  - **CSTA**, if the TSAPI Link was administered as unencrypted in **Section 5.3**.
  - **CSTA-S**, if the TSAPI Link was administered as encrypted in **Section 5.3**.
- **AE\_server\_name** represents the Application Enablement Services Server name.

## 5.5. Configure CTI Users

This section provides the steps required to configure a CTI user. If necessary, log in to the Application Enablement Services server again with the appropriate credentials for accessing the “User Management” pages.

1. Navigate to the “OAM Home” page. Select **User Management** from the left pane menu.



2. Navigate to the **User Management > Add User**. On the “Add User” page, provide the following information:

- In the **User Id** field, type the user ID being assigned to the user.
- In the **Common Name** field, enter the name the user prefers to use.
- In the **Surname** field, type the surname.
- In the **User Password** field, type the password being assigned to the user.
- In the **Confirm Password** field, re-type the assigned password.
- In the **CT User field**, select **Yes** to add the user as a member of the Security Database (SDB).

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

**AVAYA** Application Enablement Services  
Operations Administration and Maintenance

[OAM Home](#) [Help](#) [Logout](#)

**User Management Home** You are here: > [User Management](#) > [Add User](#)

**Add User**

Fields marked with \* can not be empty.

\* User Id

\* Common Name

\* Surname

\* User Password

\* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Cms Home

CT User

Department Number

3. Select **OAM Home** in upper right and navigate to the **CTI OAM Administration** → **Security Database** → **CTI Users** → **List All Users** page. Select the **User ID** created in **Step 2**, and click the **Edit** button to set the permissions of the user.

The screenshot shows the Avaya Application Enablement Services interface. The breadcrumb trail is: Administration > Security Database > CTI Users > List All Users. The main content area displays a table of CTI Users:

	User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/>	DevConnect	DevConnect	NONE	NONE
<input type="radio"/>	test0	test0	NONE	NONE
<input type="radio"/>	test1	test1	NONE	NONE
<input type="radio"/>	test2	test2	NONE	NONE
<input type="radio"/>	test3	test3	NONE	NONE
<input type="radio"/>	test4	test4	NONE	NONE
<input type="radio"/>	test5	test5	NONE	NONE
<input type="radio"/>	test6	test6	NONE	NONE
<input type="radio"/>	test7	test7	NONE	NONE
<input type="radio"/>	test8	test8	NONE	NONE
<input type="radio"/>	test9	test9	NONE	NONE

At the bottom of the table, there are two buttons: **Edit** and **List All**. The **Edit** button is highlighted with a red box.

4. Provide the user with unrestricted access privileges by clicking the **Enable** button on the **Unrestricted Access** field. A Warning screen will be displayed (not shown). Click **Apply**.

The screenshot shows the Avaya Application Enablement Services interface for editing a CTI user. The breadcrumb trail is: Administration > Security Database > CTI Users > List All Users. The main content area displays the 'Edit CTI User' form:

User ID: DevConnect  
 Common Name: DevConnect  
 Worktop Name: NONE (dropdown menu)  
 Unrestricted Access: **Enable** (button, highlighted with a red box)  
 Call Origination and Termination: None (dropdown menu)  
 Device / Device: None (dropdown menu)  
 Call / Device: None (dropdown menu)  
 Call / Call:   
 Allow Routing on Listed Device: None (dropdown menu)  
 Apply Changes (button)    Cancel (button)

## 6. Configure OnviSource OnviCord

This section describes the configuration required for the OnviSource OnviCord server to interface with Application Enablement Services and Communication Manager.

### 6.1. Configure IMA Manager to run as a Plugin

The Integra Media Adapter (IMA) Manager provides access to data related to IMA service. The IMA Manager runs as a plug-in to OnViews. To configure OnViews to run the IMA Manager, the Plugins.xml file must be modified. The file can be located by browsing to: C:\Program Files\OnviSource\OnviCenter on the OnviSource server. The section bolded and highlighted in yellow below must be added.

```
<Plugins>
  <WebPlugins>
    <Item>
      <Name>OnviCord Web</Name>
      <Description>Review and manage recording information, manage system
configuration</Description>
      <Version>6.1.3.0</Version>
      <Help>OnviCord Web.chm</Help>
      <Link>http://localhost/login.asp</Link>
      <Image>OnviCordWeb.png</Image>
    </Item>
  </WebPlugins>

  <ExePlugins>
    <Item>
      <Name>OnviCord Monitor</Name>
      <Description>Live monitor recordings</Description>
      <Version>6.1.3.0</Version>
      <Help>OnviCordMonitor.chm</Help>
      <Exe>OnviCordMonitor.exe</Exe>
      <Image>OnviCordMonitor.png</Image>
    </Item>
  </ExePlugins>

  <DllPlugins>
    <Item>
      <Name>Manager</Name>
      <Help>Manager.chm</Help>
      <AllowMultiple>>false</AllowMultiple>
    </Item>
    <Item>
      <Name>IMA_Manager</Name>
      <Help></Help>
      <AllowMultiple>>false</AllowMultiple>
    </Item>
    <Item>
      <Name>Message Server</Name>
      <Help>MessageServer.chm</Help>
```

```
<AllowMultiple>true</AllowMultiple>
</Item>
</DllPlugins>
</Plugins>
```

## 6.2. Configure Link to AES and Communication Manger

To configure the IMA Service for use with Application Enablement Services and Communication Manager, open the App.config file located in the directory where the IMA service was installed. Edit the file to provide the following information:

- Database Settings
  - **DatabaseName:** The name of your OnviSource Database. The default is OnviCenter.
  - **DbPassword:** The encrypted password for the Database. This will be provided by OnviSource.
- AES Configuration
  - **AvayaSessionUserName:** Enter the **User ID** administered in **Section 5.5**.
  - **AvayaUserPassword:** Enter the **Password** administered in **Section 5.5**.
  - **AvayaServiceProviderIP:** Enter the IP address of the Application Enablement Services server.
  - **DataServerIP:** Enter the IP address of the OnviSource DB. During compliance testing, the OnviSource DB was located on the OnviSource Server.
  - **MediaIP:** Enter the Recording Server IP address for Communication Manager to send RTP traffic. During compliance testing, the OnviSource DB was located on the OnviSource Server.
  - **DefaultAvayaSwitchName:** Enter the switch **Connection Name** administered in **Section 5.1**.
  - **GroupName:** This field is used when assigning groups to extensions in a multisite environment.
  - **CaptureMode:** Enter **2**. The following options are available:
    - 1=Display Only
    - 2= Display and Media
    - 3=Media Only
    - 4=Call Control Only
  - **CtiLinkName:** Enter the **Connection Name** administered in **Section 5.1**.

```

<!-- ===== Database Settings ===== -->
<add key="DatabaseName" value="OnviCenter"/> <!-- OnviCenter
<add key="DbPassword" value="kAQFILcodGvNINP1RNB2li05LBIRFHJe"/>

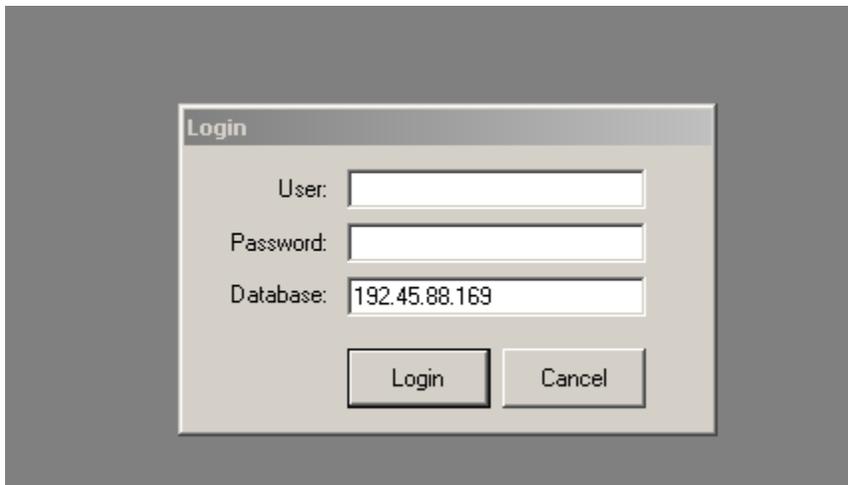
<!-- AvayaServiceProviderIP value="192.45.88.25"
<add key="AvayaSessionUserName" value="DevConnect"/>
<add key="AvayaUserPassword" value="DevConnect123."/>
<add key="AvayaServiceProviderIP" value="192.45.88.25"/>
<add key="DataServerIP" value="192.45.88.169"/>
<add key="MediaIP" value="192.45.88.169"/>
<add key="DataServerIP" value="localhost"/>
<add key="MediaIP" value="localhost"/>
<add key="DefaultAvayaSwitchName" value="8500"/>
<add key="GroupName" value="AMALAB"/>
<add key="CaptureMode" value="2"/>
<add key="CtiLinkName" value="8500"/>
-->

```

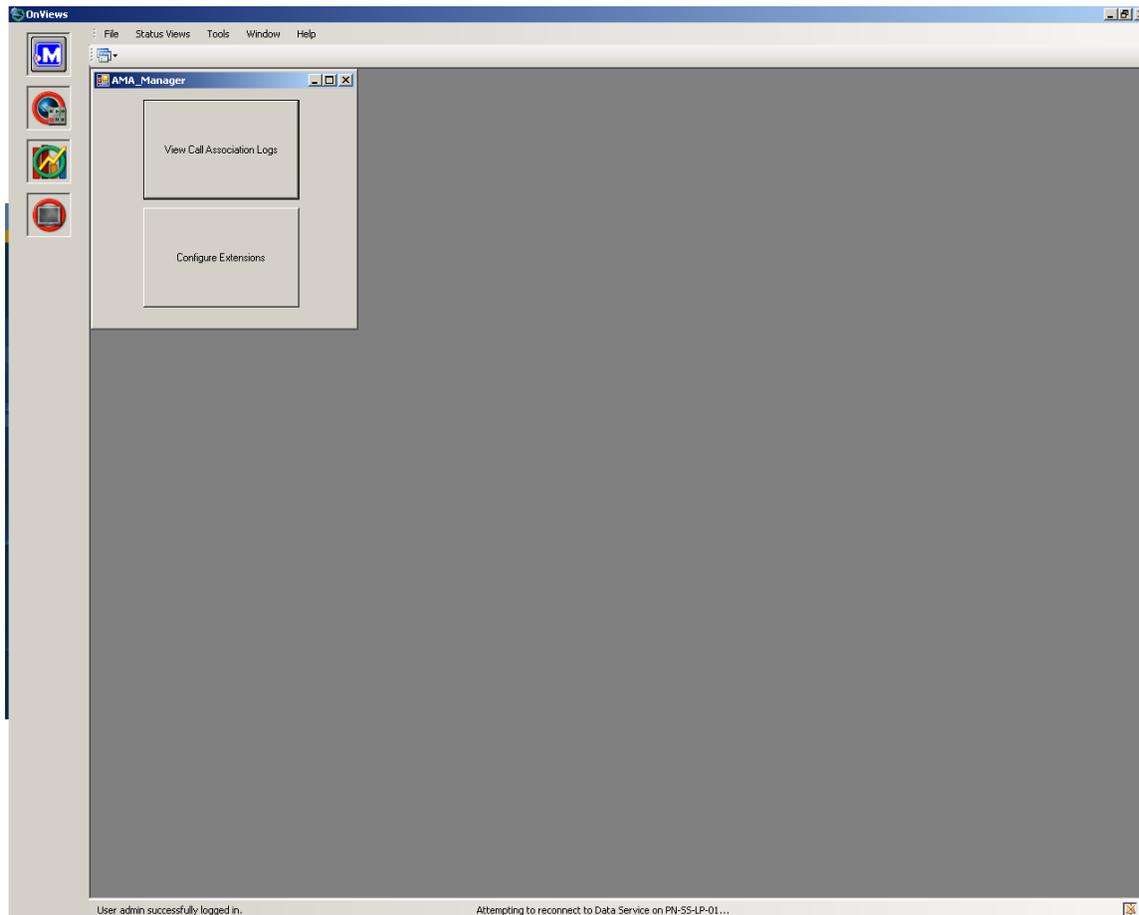
### 6.3. Accessing the IMA manager

The IMA manager can be accessed through the OnViews management console on the OnviSource Server.

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

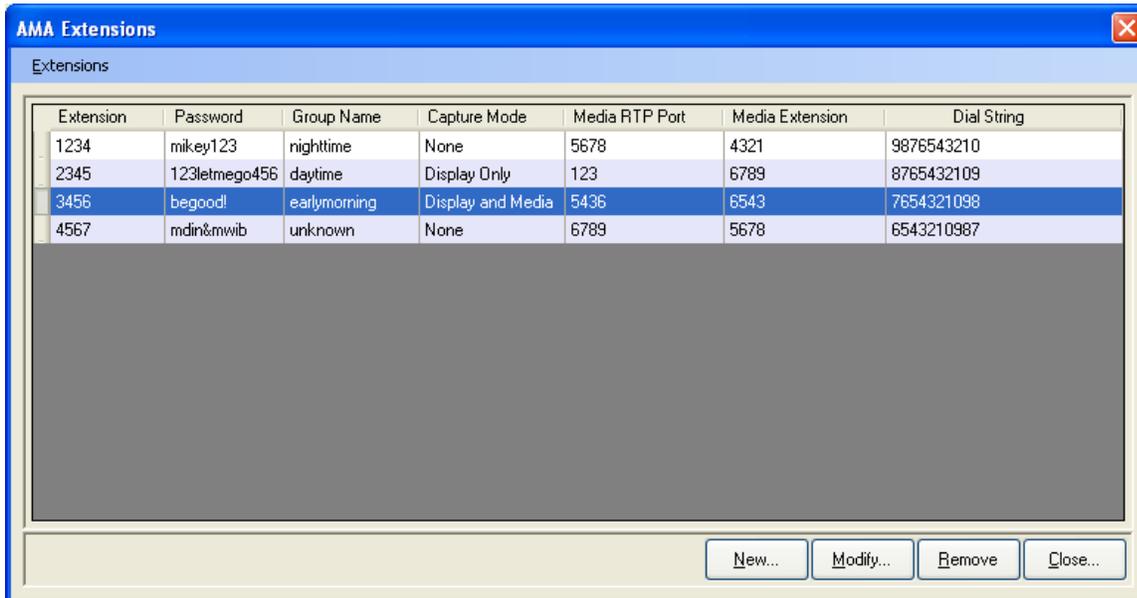


The IMA manager application can be launched by clicking the appropriate icon on the left menu bar.



## 6.4. Administer Devices for Recording

To configure the IMA/IMA service, press the **Configure Extensions** button on the main screen. A new dialog, similar to the one below appears.

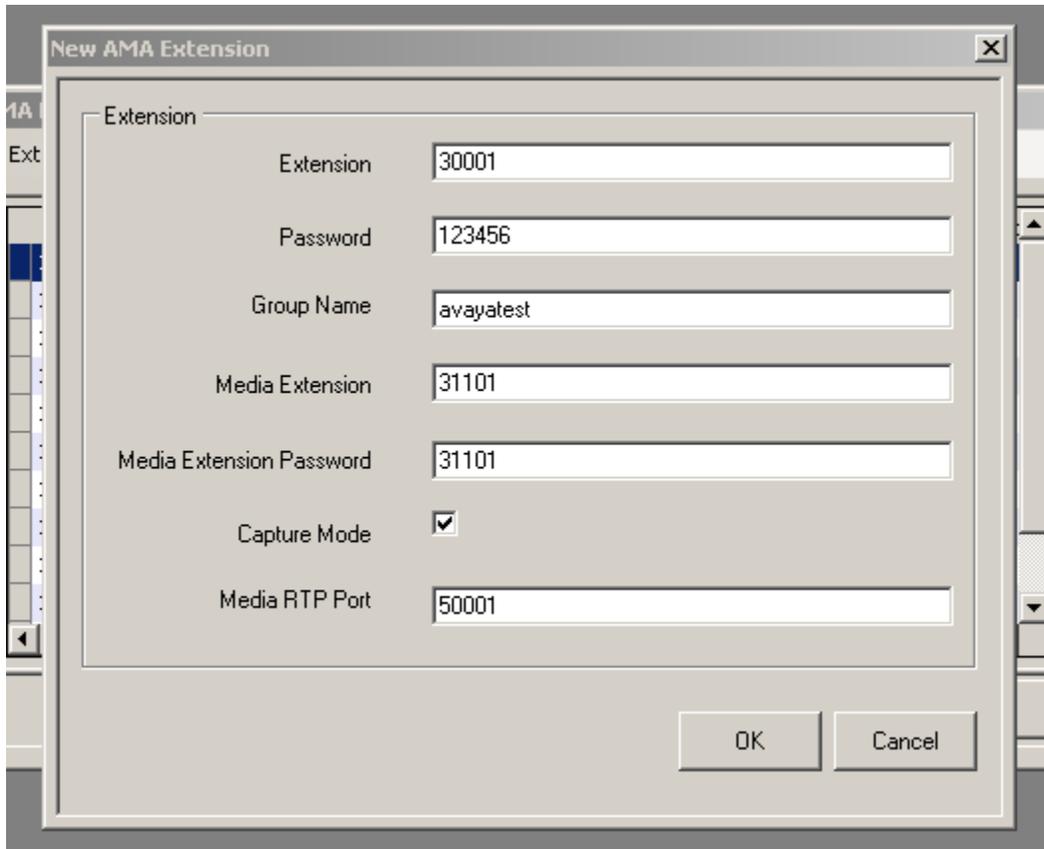


Each row in the table represents a single extension defined within the database that controls the behavior of the IMA/IMA service. To add a new extension, click the **New** button and provide the following information:

- **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 4.4**, used to capture audio media for calls to the primary extension.
- **Capture Mode:** Determines specifically what will be captured for the extension. The options are: None, Display only, and Media and Display. This value should correspond to

the Capture mode as specified in the configuration file for the service responsible for the extension. Otherwise, nothing will be captured for the extension.

- **Media Extension Password:** Enter the password associated with the DMCC recording device, as configured on Communication Manager.
- **Media RTP Port:** Enter the IP port to which audio media for the extension will be sent. Although an odd port was used for this test in the lab, Avaya recommends the use of even ports for the Media RTP Port..
- **Dial string:** This field exists for backwards compatibility. It is not used for current versions of IMA/IMA.



The screenshot shows a dialog box titled "New AMA Extension". It contains the following fields and values:

Field	Value
Extension	30001
Password	123456
Group Name	avayatest
Media Extension	31101
Media Extension Password	31101
Capture Mode	<input checked="" type="checkbox"/>
Media RTP Port	50001

Buttons: OK, Cancel

Click **OK** to save changes.

## 7. General Test Approach and Test Results

The general test approach was to place calls and use basic telephony operations to verify that OnviSource OnviCord could properly record the calls, associate the calls with the correct stations and agents, and to confirm that quality recordings could be retrieved and played back. The test cases were broken down into three categories: feature testing, serviceability testing, and performance testing.

For feature testing, several types of calls were placed, including:

- Internal calls
- Inbound trunk calls
- Outbound trunk calls
- Transfer and Conference calls

The calls were placed to and from various endpoints, including: stations, agents, VDNs, and hunt groups.

For serviceability testing, failure conditions were introduced into the test configuration, such as network cable pulls, CTI link busyouts, and server resets to verify that OnviSource OnviCord could properly resume operation after failure recovery.

For performance testing, a sustained volume of calls were generated for an extended period of time to verify that OnviSource OnviCord could record all the calls during that time period.

All test cases were executed and passed.

## 8. Verification Steps

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

### 8.1. Verify Communication Manager

This section provides the steps required to verify the status of the link(s) to Application Enablement Services and the CTI link.

1. Enter the **status aesvcs link** command. Verify the **Remote IP** is the IP address of the Application Enablement Services server, the **Local Node** displays each CLAN used for connectivity to Application Enablement Services, and that there is appropriate message traffic over the links (**Msgs Sent** and **Msgs Rcvd**).

```
status aesvcs link
```

AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	aeserver25	192. 45. 88. 25	56300	CLAN2	207	192
01/02	aeserver25	192. 45. 88. 25	56302	CLAN4	180	180
01/03	aeserver25	192. 45. 88. 25	56304	CLAN3	180	180

1. Enter the **status aesvcs cti-link** command. Verify the **Service State** is **established** for the CTI link number administered in **Section 4.3**.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	<b>Service State</b>	Msgs Sent	Msgs Rcvd
1		no		down	0	0
2		no		down	0	0
3		no		down	0	0
4		no		down	0	0
5		no		down	0	0
6		no		down	0	0
7		no		down	0	0
8		no		down	0	0
9		no		down	0	0
<b>10</b>	<b>4</b>	<b>no</b>	<b>aeserver25</b>	<b>established</b>	<b>15</b>	<b>15</b>

## 8.2. Verify Application Enablement Services

This section provides the steps required to verify the status of the TSAPI and DMCC services.

1. From the Application Enablement Services “CTI OAM Admin” web pages, navigate to **Status and Control > Services Summary** in the left pane menu. Verify that the **State** of the **TSAPI Service** and the **DMCC Service** is **ONLINE**.

The screenshot shows the Avaya Application Enablement Services web interface. The left navigation pane is expanded to 'Status and Control', and 'Services Summary' is selected. The main content area displays a table of services with the following data:

Service	State	Since	Cause
<input type="radio"/> CVLAN Service	ONLINE	2009-03-24 09:58:23	NORMAL
<input type="radio"/> DLG Service	ONLINE	2009-03-24 09:58:20	NORMAL
<input checked="" type="radio"/> TSAPI Service	ONLINE	2009-03-24 09:58:24	NORMAL
<input type="radio"/> DMCC Service	ONLINE	2009-03-24 09:58:25	NORMAL

A 'Details' button is located below the table.

2. Select the radio button for **TSAPI Service**, and click **Details**.

This screenshot is identical to the previous one, but with the 'Details' button highlighted with a red box, indicating the next step in the process.

3. Verify that the **Conn Status** is **Talking** for the TSAPI link administered in **Section 5.3**.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The top header displays the Avaya logo and the title "Application Enablement Services" with the subtitle "Operations Administration and Maintenance". A breadcrumb trail indicates the current location: "You are here: > Status and Control > Services Summary".

The left navigation menu includes the following items:
 

- CTI OAM Home
- Administration
- Status and Control
  - Switch Conn Summary
  - Services Summary
- Maintenance
- Alarms
- Logs
- Utilities
- Help

The main content area is titled "TSAPI Link Details" and contains a table with the following data:

Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
1	8500	10	Talking	2009-03-24 09:58:23.0	Online	15	0	16
2	8300	10	Talking	2009-03-24 09:58:23.0	Online	15	0	16

### 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 the OnviSource OnviCord Client PC, right-click on the square icon in your system tray, then select **OnviCord Web** from the popup menu. To log into "OnviCord Web" from OnViews, click the **OnviCord Web** icon in the Toolbar OR select **Tools-> OnviCord Web** from the menu bar.

**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".

The screenshot shows a login form with the following elements:
 

- Login** (Section Header)
- User:** [User ID (usually initials)]
- Password:** [\*\*\*\*\*]
- Login** (Button)

- 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.

Home | **Recent Recordings** | Search | Reports | Evaluate | Messages | Outbox | Manage | [logout](#) | [help](#)

Welcome **Administrator**  
 Logged IP: 172.20.1.87  
 Password set June 8th, 2006

Dates: Month / Day / Year | 12 hour  
 Names: LastName, FirstName

**Personal settings**

Photo:

First name:

Last name:

Email:

Password:

Verify:

**System statistics for June 13th, 2006**

**ALL RECORDINGS**  
 Total recordings: 0  
 Total time: 00:00:00  
 Average length: 00:00:00

**1 MINUTE OR LONGER**  
 Total recordings: 0  
 Total time: 00:00:00  
 Average length: 00:00:00

**RECORDING HISTORY**  
 Played recordings: 0  
 Notes added: 0  
 Evaluations completed: 0  
 Files attached: 0  
 Color codes added: 0  
 Flags added: 0  
 Sent records: 0

Copyright © 2006 OnviSource, Inc.  
 Email info@onvisource.com

**OnviSource**

- 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 number of recent recordings (a range between 10 recordings to an unlimited maximum).

Home | **Recent Recordings** | Search | Reports | Evaluate | Messages | Outbox | [logout](#) | [help](#)

**Recent options**

Time: 24 hours  
 Records: Unlimited  
 Refresh: None

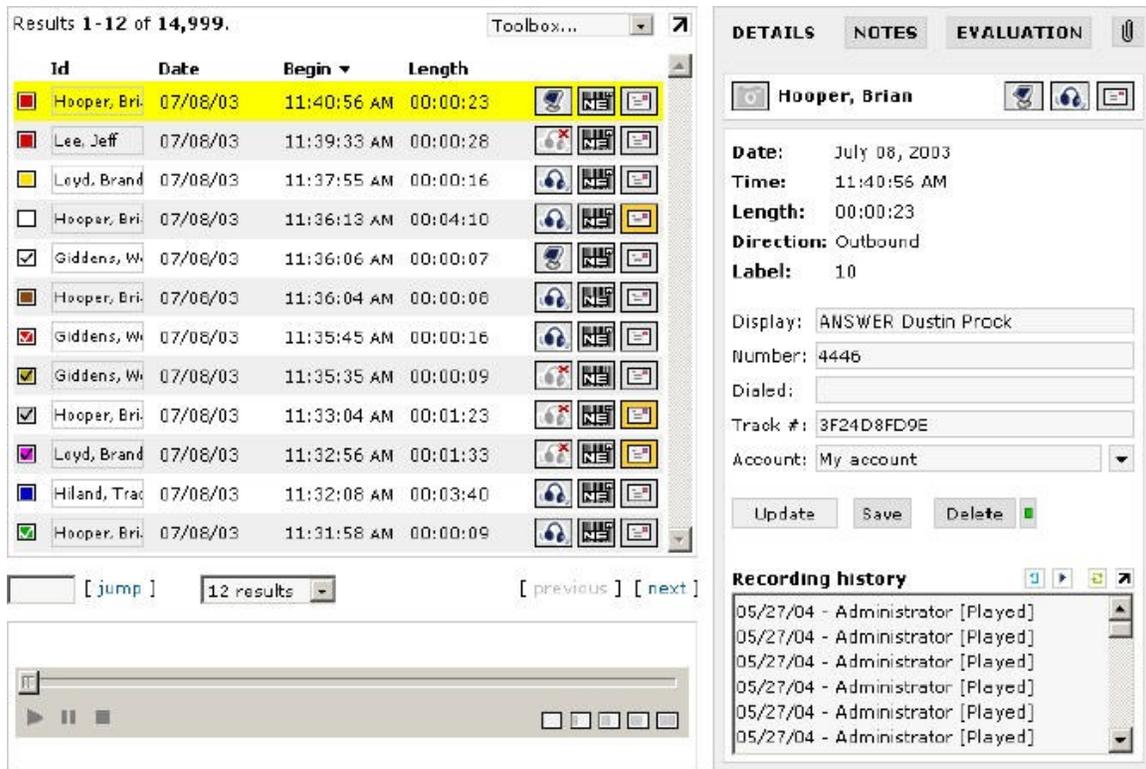
**Default columns**

Id: User name  
 First: Date  
 Second: Begin time  
 Third: Length

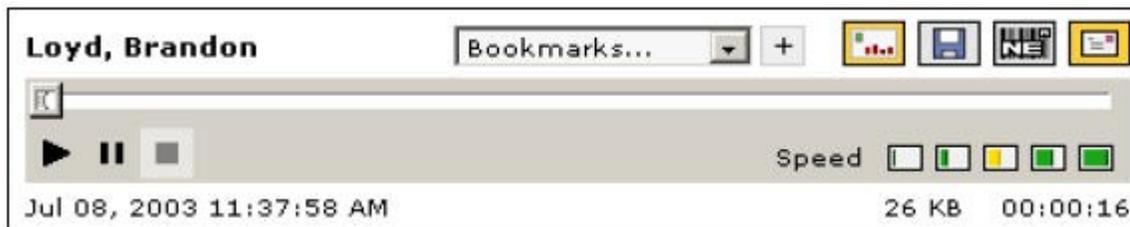
**Users and channels**

Jones, Bill

- 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.



- 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 OnviSource OnviCord 6.1.3 to interoperate with Avaya Aura™ Communication Manager 5.2 and Avaya Aura™ Application Enablement Services 4.2. All feature, serviceability, and performance test cases were completed and passed.

## 10. Additional References

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

The following Avaya product documentation can be found at <http://support.avaya.com>:

[1] *Administering Avaya Aura™ Communication Manager*, Doc ID: 03-300509, Issue 5.0, Release 5.2, May 2009

[2] *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*, Doc ID: 02-300357, Release 4.2, Issue 10, May 2008

OnviSource product documentation can be obtained by contacting OnviSource's customer support: <http://www.onvisource.com/support/index.php>.

## 11. Change History

Issue	Date	Reason
1.1	02/12/2010	Updated Section 6.4 to state Avaya recommends the use of even ports for the Media RTP Port.
1.0	10/26/2009	Initial issue

---

**©2010 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. 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](mailto:devconnect@avaya.com).