



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

---

# **Application Notes for Presence Technology Presence Recording R10.1 with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 - Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for Presence Technology Presence Recording to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Presence Technology Presence Recording is part of the Presence Technology Presence Suite, a multi-channel contact management suite which handles voice, text chat, email and web contact mechanisms. Presence Technology Presence Recording integrates with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using single step conferencing implemented via DMCC over TSAPI.

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

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

# 1. Introduction

These Application Notes describe the compliance tested configuration using Presence Technology Presence Recording R10.1 with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 (AES).

Presence Technology Presence Recording is a component of Presence Technology Presence Suite, a multi-channel contact management suite able to handle voice, e-mail and web chat contact mechanisms. Presence Technology Presence Recording uses Avaya Aura® Communication Manager's Single Step Conferencing (SSC) feature via the Device, Media and Call Control (DMCC) service provided by Avaya Aura® Application Enablement Services (AES) to capture the audio and call details for recording agent calls. Presence Technology Presence Recording uses the Avaya Aura® Application Enablement Services DMCC service to register a pool of virtual IP softphones that are used as "recorders". Target agents, whose calls are to be recorded, are configured in the Presence Technology Presence Recording administration tool. When a target agent places or receives a call, SSC is used to conference in a "recorder" to capture the audio stream and call details.

## 2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of Presence Recording to carry out call recording in a variety of scenarios using DMCC with AES and Communication Manager.

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

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- Call Hold
- Drop
- Blind Transfer
- Consultative Transfer
- Blind 3-way Conference
- Supervised Conference
- Bridged Appearances
- Intra switch call
- Inbound trunk call
- Outbound trunk call
- Malicious Call
- Multiple simultaneous calls
- No Answer, Engaged, Unobtainable
- Fax, Answering Machine
- Manual call clear

The serviceability testing focused on verifying the ability of Presence Recording to recover from disconnection and reconnection to the Avaya solution.

## 2.2. Test Results

All functionality and serviceability test cases were completed successfully.

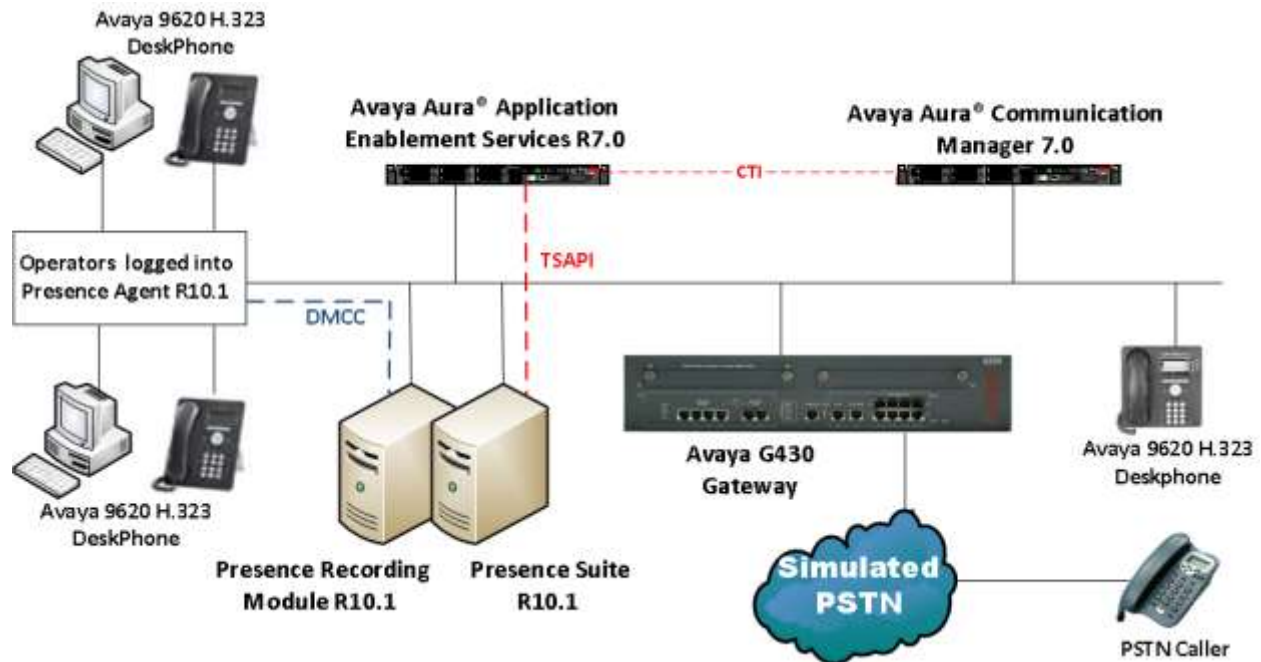
## 2.3. Support

Technical support can be obtained for Presence Technology Presence Suite as follows:

- Email: [support@presenceco.com](mailto:support@presenceco.com)
- Website: [www.presenceco.com](http://www.presenceco.com)
- Phone: +34 93 10 10 300

### 3. Reference Configuration

**Figure 1** shows the network topology during interoperability testing. VMWare Virtual Machine running Communication Manager with an Avaya G430 Media Gateway was used as the hosting PBX. Presence Suite with the Presence Recording component and Presence Agent PC's are connected to the LAN and recording is performed using the Single Step Conference feature of Communication Manager using DMCC provided by AES.



**Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services, and Presence Technology Presence Suite Server with Presence Recording component configuration**

## 4. Equipment and Software Validated

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

• Equipment/Software	• Release/Version
Avaya Aura® Communication Manager running on VMWare Virtual Machine	R7.0 SP1 Revision 7.0.0.1.0.441.22438
Avaya Aura® Application Enablement Services running on VMWare Virtual Machine	R7.0 Build No – 7.0.0.0.0.13-0
Avaya G430 Media Gateway	FW 37.19.0
Avaya 96xx Series Deskphone	3.2 SP3 (H.323)
Presence Server and Presence Recording Server running on Windows Server 2008 R2	R10.1
Presence Client running on Windows 7 SP1 and Windows Server 2008 R2	R10.1

## 5. Configure Avaya Aura® Communication Manager

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

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT). Please note that this is the setup required to add the Presence Recording only the setup of the other possible Presence Suite is outside the scope of these Application Notes but can be found in the Application Notes titled *Application Notes for Configuring Presence Technology Presence Suite R10.1 with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0*.

### 5.1. Verify System Features

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

display system-parameters customer-options		Page	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
<b>Answer Supervision by Call Classifier?</b>	<b>y</b>	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
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	Digital Loss Plan Modification?	y	
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y	
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y	
ATMS?	y			
Attendant Vectoring?	y			

## 5.2. Note IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP Address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes63vmpg**).

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM100	10.10.40.34	
<b>AES71678</b>	<b>10.10.40.30</b>	
default	0.0.0.0	
g430	10.10.40.15	
<b>procr</b>	<b>10.10.40.31</b>	

## 5.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** should be set to **AESVCS**.
- **Enabled:** set to **y**.
- **Local Node:** set to the node name assigned for the procr in **Section 5.10**.
- **Local Port** Retain the default value of **8765**.

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

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **AES71678**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

**Note:** The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services					Page 4 of 4
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	<b>AES71678</b>	*****	<b>y</b>	idle	
2:					
3:					

## 5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. 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: 2002
      Type: ADJ-IP
                                         COR: 1
Name: AES71678
```

## 5.5. Configure Recorder/Playback Pool Stations

Presence Recording uses the Single Step Conferencing method to conference “recorders” with the agent calls in order to capture the call audio. Use the command **add station** to configure a station for each of the recording pool stations. On **Page 1** enter a descriptive **Name** and **Security Code**, set the **Port** to **IP**, set the **Type** to **4624** and set **IP SoftPhone** to **y**. Repeat according to the maximum number of call to be recorded simultaneously. These extensions can also be configured on Presence Recording for the playback of recordings. Configure sufficient stations to accommodate for the maximum number of simultaneous recording playback channels required.

```
add station 8270400                               Page   1 of   6
                                         STATION
Extension: 8270400      Lock Messages? n          BCC: 0
      Type: 4624        Security Code: 1234        TN: 1
      Port: IP          Coverage Path 1:          COR: 1
      Name: Presenceco Recorder 1      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: 1591
Survivable GK Node Name:      Mute Button Enabled? y
      Survivable COR: internal      Media Complex Ext:
      Survivable Trunk Dest? y      IP SoftPhone? y
                                         IP Video Softphone? n
```



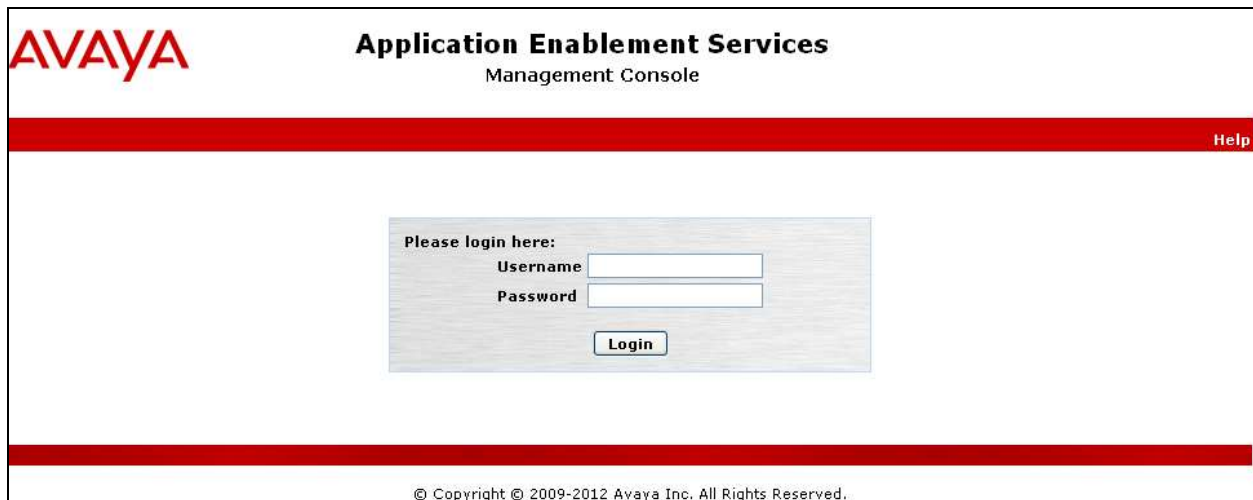
## 6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Enable CTI Link User
- Identify Tlinks

### 6.1. Verify Licensing

To access the maintenance console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the active IP address of AES. The login screen is displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a "Login" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." is displayed.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

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

## 6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter in a name for the Switch Connection to be added and click the **Add Connection** button.

In the resulting screen enter the **Switch Password**, the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.11**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the procr as shown in **Section 5.10** that will be used for the AES connection and select the **Add Name or IP** button.

### 6.3. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.

On the **Add TSAPI Links** screen, enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM1627**, which has already been configured in **Section 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **7**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.

Another screen appears for confirmation of the changes. Choose **Apply**.

**Apply Changes to Link**  

Warning! Are you sure you want to apply the changes?  
These changes can only take effect when the TSAPI server restarts.  
Please use the Maintenance -> Service Controller page to restart the TSAPI server.

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

**Service Controller**

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

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

## 6.4. Create Avaya CTI User

A User ID and password needs to be configured for the Presence Suite server to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option (not shown). In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the Presence Suite Server in **Section 7.1**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **User Id** in **Section 7.1**.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen (not shown).

The screenshot shows the 'Edit User' form in the Avaya User Management interface. The form is titled 'Edit User' and contains several input fields. A red box highlights the 'User Id', 'Common Name', and 'Surname' fields, which are all set to 'presence'. Another red box highlights the 'CT User' dropdown menu, which is set to 'Yes'. The left sidebar shows the navigation menu with 'User Admin' selected.

The next screen will show a message indicating that the user was created successfully (not shown).

## 6.5. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 6.4** and select the **Edit** option (not shown). The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

The screenshot shows the 'Edit CTI User' form in the Avaya Security Database interface. The form is titled 'Edit CTI User' and contains several sections. A red box highlights the 'Unrestricted Access' checkbox, which is checked. The left sidebar shows the navigation menu with 'Security Database' selected.

A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

## 6.6. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Presence Suite in **Section 7.1**.

The screenshot displays the Avaya Management System (AMS) interface. On the left is a navigation tree with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users, Devices, Device Groups, and Tlinks (selected). The main content area on the right is titled 'Tlinks'. It contains a 'Tlink Name' section with two radio button options: 'AVAYA#CM1627#CSTA#AES71678' (which is selected) and 'AVAYA#CM1627#CSTA-S#AES71678'. Below these options is a 'Delete Tlink' button.

## 6.7. Enable DMCC ports

In order to enable DMCC for call recording navigate to **Networking→Ports→DMCC Server Ports**.

- Enable DMCC **Unencrypted Port**
- Enable DMCC **Encrypted Port**
- Enable DMCC **TR/87 Port**

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

**Networking | Ports**

**Ports**

CVLAN Ports

			Enabled	Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	9998		<input checked="" type="radio"/>	<input type="radio"/>

DLG Port

TCP Port	
5678	

TSAPI Ports

			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	1050			
TCP Port Max	1065			
Encrypted TLINK Ports				
TCP Port Min	1066			
TCP Port Max	1081			

**DMCC Server Ports**

			Enabled	Disabled
Unencrypted Port	4721		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	4722		<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	4723		<input checked="" type="radio"/>	<input type="radio"/>

Once this change is made a restart of the AE Server is required. Navigate to **Maintenance → Service Controller**. In the main screen select **Restart AE Server** highlighted.

**AVAYA** Application Enablement Services Management Console

**Maintenance | Service Controller**

**Service Controller**

Service	Controller Status
<input type="checkbox"/> ASAL Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

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

## 7. Configure Presence Recording

The Presence Recording can be an additional component of Presence Suite but may also be installed as a stand-alone product. These Application Notes will show the configuration for both instances in both cases the Presence Recording Server must be configured to connect with AES.

The Presence Suite includes the Presence Server, Presence Mail Interactions Server, Presence Web Interactions Server, Presence Administrator, Presence Supervisor, and Presence Agent. The Presence server was configured and provided by Presence Technology. The setup of Presence Server is outside the scope of these Application Notes but can be found in the Application Notes titled *Application Notes for Configuring Presence Technology Presence Suite R10.1 with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0*.

### 7.1. Configure Telephony, Storage and CTI Parameters

From the Presence server, navigate to **C:\Presence\** and double click on **precservercfg.exe** (not shown), the screen below will appear. In the **Ports** section, configure a **Recording Server** port; enter the **IP address** of the Presence Server and the port used for connection. Tick the **Integrated with Presence Server** box if the Presence server has been installed and select **DMCC extensions** from the **Channel type** drop-down box.

**Note:** If the Presence Server is a part of the installation the Integrated with Presence Server box is ticked and thus the CTI connection already in place for the Presence Server is used by the Presence Recording.

The screenshot shows the 'Presence Recording Server Configuration' dialog box with the 'General' tab selected. The left sidebar lists various configuration categories: General, Backup servers, Storage, Channels, Alerts, Tracing, Server, Backup Server, Service, Screen Recording, General, and Tracing. The main area contains the following settings:

- ☐ Configure Recording Server as slave
- Ports:**
  - Recording Server: 6111
  - Backup Recording Server: 6120
- Presence Server:**
  - ☒ Integrated with Presence Server (highlighted with a red box)
  - IP address: 10.10.16.127
  - Port: 6100
  - ☐ Enable Recording Server as unified server: Main
- Channel type:** DMCC extensions (highlighted with a red box)
- Audio format: G711 (a-Law/u-Law)
- Maximum recording duration (in seconds): 0
- ☐ Encrypt recording files

At the bottom are 'OK' and 'Cancel' buttons.



### 7.1.1. Configure the CTI Connection

If the CTI connection is not in place select the **Primary link** menu on the left side of the screen and choose the **Edit** button to enter a value.

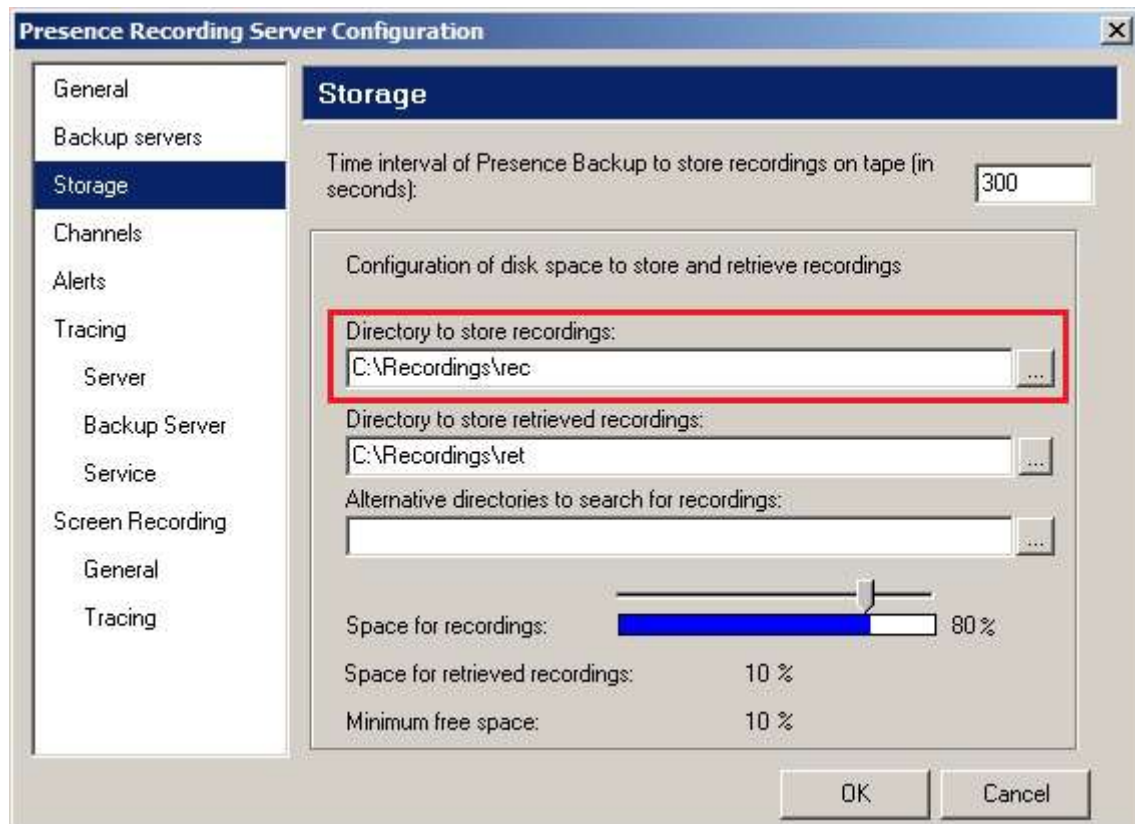
The image shows the 'Presence Server Configuration' dialog box with the 'Primary link' tab selected. The left sidebar lists various configuration categories: Identification, Database, Authentication, General, Switch, Primary link (highlighted), Outbound links, Servers, License, Alarms, Tracing, Statistics Server, Storage, Inbound, Internet, and Tracing. The main area of the dialog has a title bar 'Primary link' and a descriptive text: 'You must specify a primary CTI link which will be used as default link. You may specify backup primary links in case that the primary link is down.' Below this, there is a 'Primary link:' label followed by a text field containing 'AVAYA#CM1627#CSTA#AES71678'. To the right of this field is a red-bordered 'Edit' button. Below the primary link field is a section titled 'List of backup links' which contains a table with one header 'CTI link name' and an empty body. To the right of the table are 'Up ↑' and 'Down ↓' buttons. Below the table are 'Add', 'Edit', and 'Remove' buttons. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

In the resulting pop-up box enter the Tlink name from **Section 6.6** in the **Name** field. For the **User** and **Password** fields enter the user name and password configured on the Application Enablement Services in **Section 6.4**. Click **OK**.

The image shows the 'Primary CTI link data' dialog box. It has a title bar 'Primary CTI link data' and a section titled 'CTI link configuration data'. Inside this section are three fields: 'Name:' with the value 'AVAYA#CM1627#CSTA#AES71678', 'User:' with the value 'presence', and 'Password:' with the value 'xxxxxxx'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

### 7.1.2. Configure Storage

Click on **Storage** in the left-hand pane and enter an appropriate directory in the **Director to store recordings** field.



### 7.1.3. Configure Telephony

Click on **Channels** in the left-hand pane. In the **DMCC Server** section, enter the IP address of the AES server and the AES user configured for the Presence Suite installation, enter the port configured for connectivity to AES (the default is **4721**). In the **DMCC channel configuration** section, click **Add**.

The screenshot shows the 'Presence Recording Server Configuration' dialog box with the 'Channels' tab selected. The left-hand pane lists various configuration categories, with 'Channels' highlighted. The main area is divided into two sections: 'DMCC Server' and 'DMCC channel configuration'. The 'DMCC Server' section contains fields for 'IP address' (10.10.16.78), 'Port' (4721), 'User' (presence), and 'Password' (masked with asterisks). The 'DMCC channel configuration' section includes a 'Base port to receive RTP packets' field (50000) and a table with columns 'Extension', 'Usage', and 'CLAN IP address'. Below the table are 'Up' and 'Down' buttons. At the bottom of the dialog are 'Add', 'Edit', and 'Remove' buttons, with the 'Add' button highlighted by a red box. The 'OK' and 'Cancel' buttons are at the bottom right.

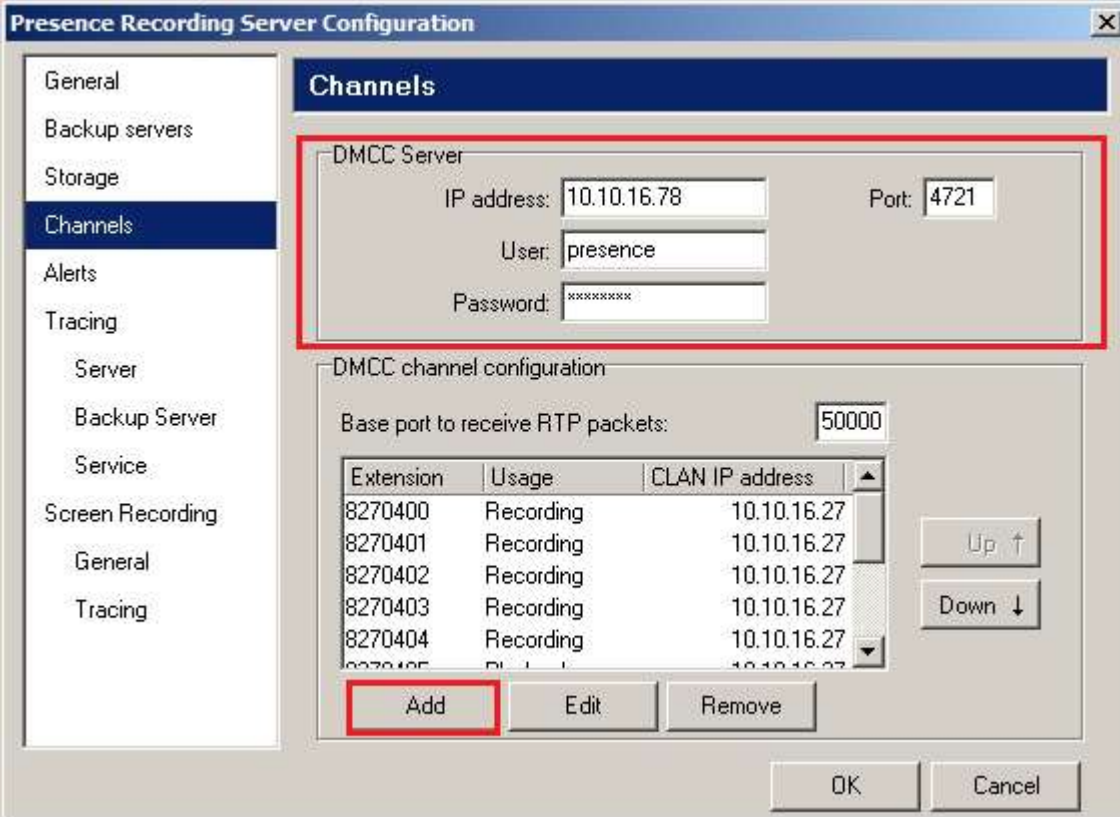
Extension	Usage	CLAN IP address
-----------	-------	-----------------

Enter a valid recording channel **Extension** and **Password** as configured in **Section 5.1**. Enter the **CLAN IP address** and select **Recording** from the **Usage** drop-down box. Click **OK** when done. Repeat as necessary. For playback channels, select **Playback** from the **Usage** drop-down box.

The screenshot displays the 'Presence Recording Server Configuration' window. The 'Channels' tab is active, showing a list of channels. A 'Channel' sub-dialog is open, allowing configuration of a new channel. The sub-dialog fields are: Extension (8270400), Password (masked with 'x'), Usage (Recording), and CLAN IP address (10.10.16.27). The main dialog also shows a 'DMCC Server' section with a Port (4721) and a 'Tracing' section. At the bottom, there are 'Add', 'Edit', and 'Remove' buttons for the channel list, and 'OK' and 'Cancel' buttons for the main configuration window.

Channel	Extension	Usage	CLAN IP address
	8270400	Recording	10.10.16.27

The screen shown below will appear, displaying all recording and playback channels, click **OK** when done.



The screenshot shows the 'Presence Recording Server Configuration' window with the 'Channels' tab selected. The left sidebar lists various configuration categories, with 'Channels' highlighted. The main area is divided into two sections: 'DMCC Server' and 'DMCC channel configuration'. The 'DMCC Server' section is enclosed in a red box and contains fields for IP address (10.10.16.78), Port (4721), User (presence), and Password (masked with asterisks). The 'DMCC channel configuration' section includes a 'Base port to receive RTP packets' field set to 50000 and a table of channels. The table has columns for Extension, Usage, and CLAN IP address. Five channels are listed, all with 'Recording' usage and IP address 10.10.16.27. Below the table are 'Add', 'Edit', and 'Remove' buttons, with the 'Add' button highlighted by a red box. 'Up' and 'Down' arrow buttons are also present. At the bottom right are 'OK' and 'Cancel' buttons.

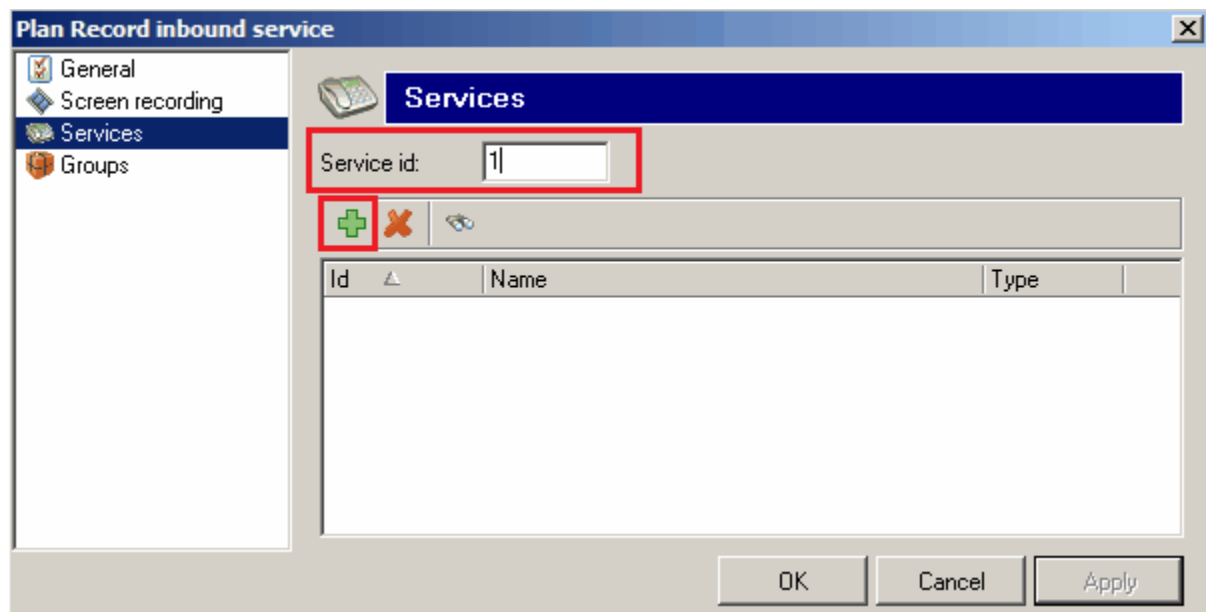
Extension	Usage	CLAN IP address
8270400	Recording	10.10.16.27
8270401	Recording	10.10.16.27
8270402	Recording	10.10.16.27
8270403	Recording	10.10.16.27
8270404	Recording	10.10.16.27

## 7.2. Configure Recording Plan

Recording plans must be configured according to the call recordings required. Using the Presence Supervisor application, click on **Recordings** → **Plans** → **New** (not shown). In the displayed **Plan Inbound service recording plan** window, assign an identifying **Name** and set the **Percentage to record** as required, in this case **100%**. Configure the **Start** and **End** parameters as appropriate.

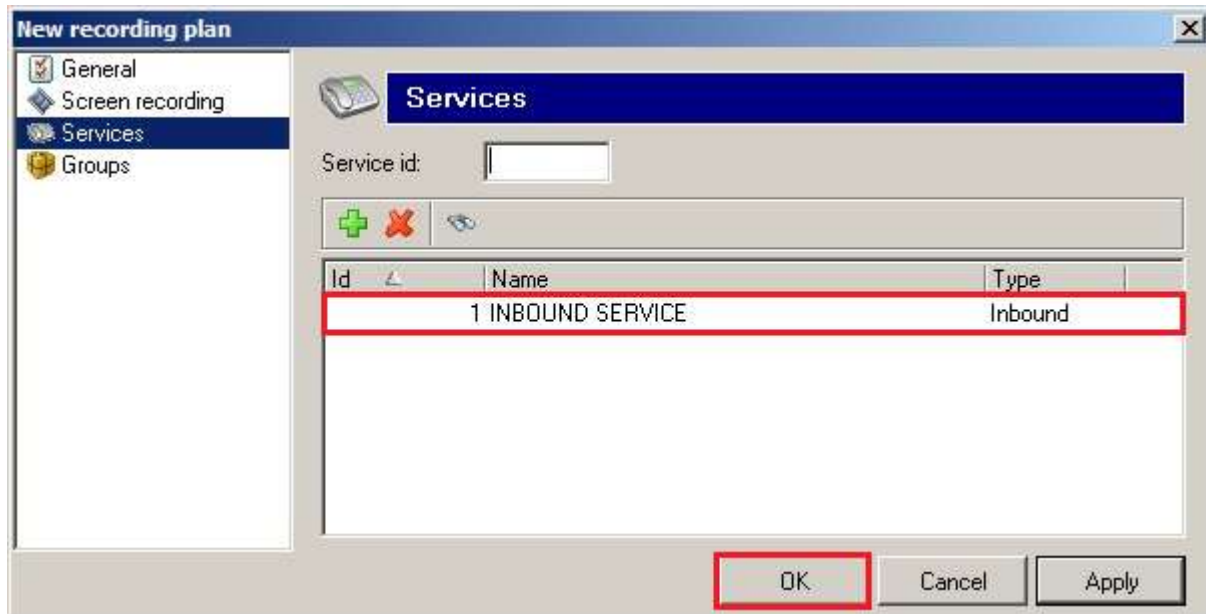


Click on **Services** in the left-hand pane, enter **1** in the **Service ID** box and click the plus icon.

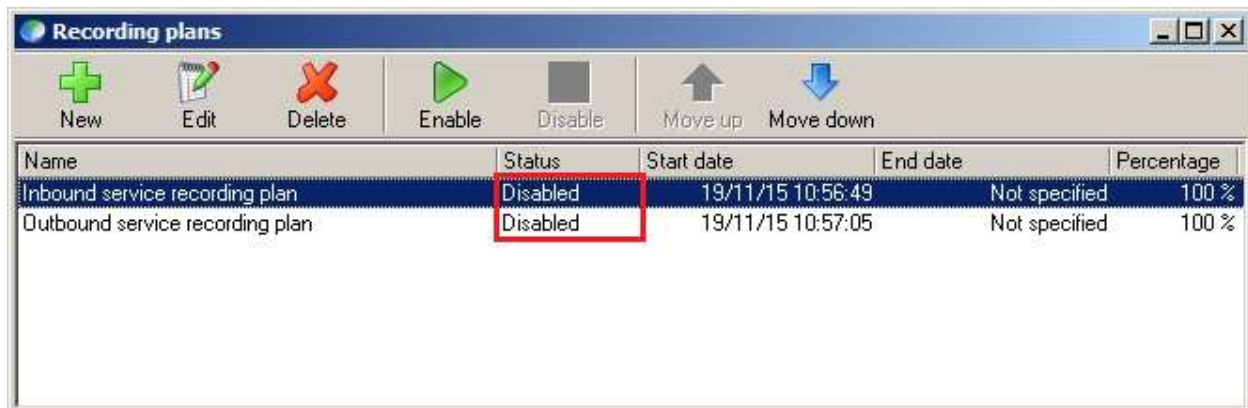


Id	Name	Type
----	------	------

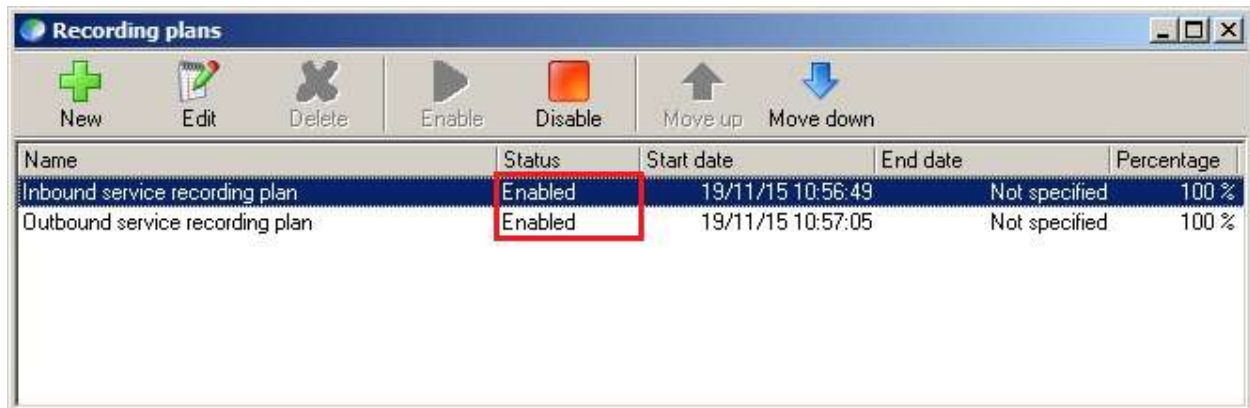
This will add the relevant configured service to the recording plan, in this case **INBOUND SERVICE**. Click **OK** when done. Repeat as necessary for additional recording plans.



The screen below will be displayed, summarizing the added recording plans. Note that the status shows **Disabled**.



Select each one in turn and click **Enable**, the status will now appear as **Enabled**.

A screenshot of a software window titled "Recording plans". The window has a toolbar with icons for "New" (green plus), "Edit" (pencil), "Delete" (X), "Enable" (play button), "Disable" (red square), "Move up" (up arrow), and "Move down" (down arrow). Below the toolbar is a table with five columns: "Name", "Status", "Start date", "End date", and "Percentage". The table contains two rows: "Inbound service recording plan" and "Outbound service recording plan". Both rows have a status of "Enabled", which is highlighted with a red rectangular box. The "Start date" for both is "19/11/15 10:56:49" and "19/11/15 10:57:05" respectively. The "End date" is "Not specified" and the "Percentage" is "100 %".

Name	Status	Start date	End date	Percentage
Inbound service recording plan	Enabled	19/11/15 10:56:49	Not specified	100 %
Outbound service recording plan	Enabled	19/11/15 10:57:05	Not specified	100 %

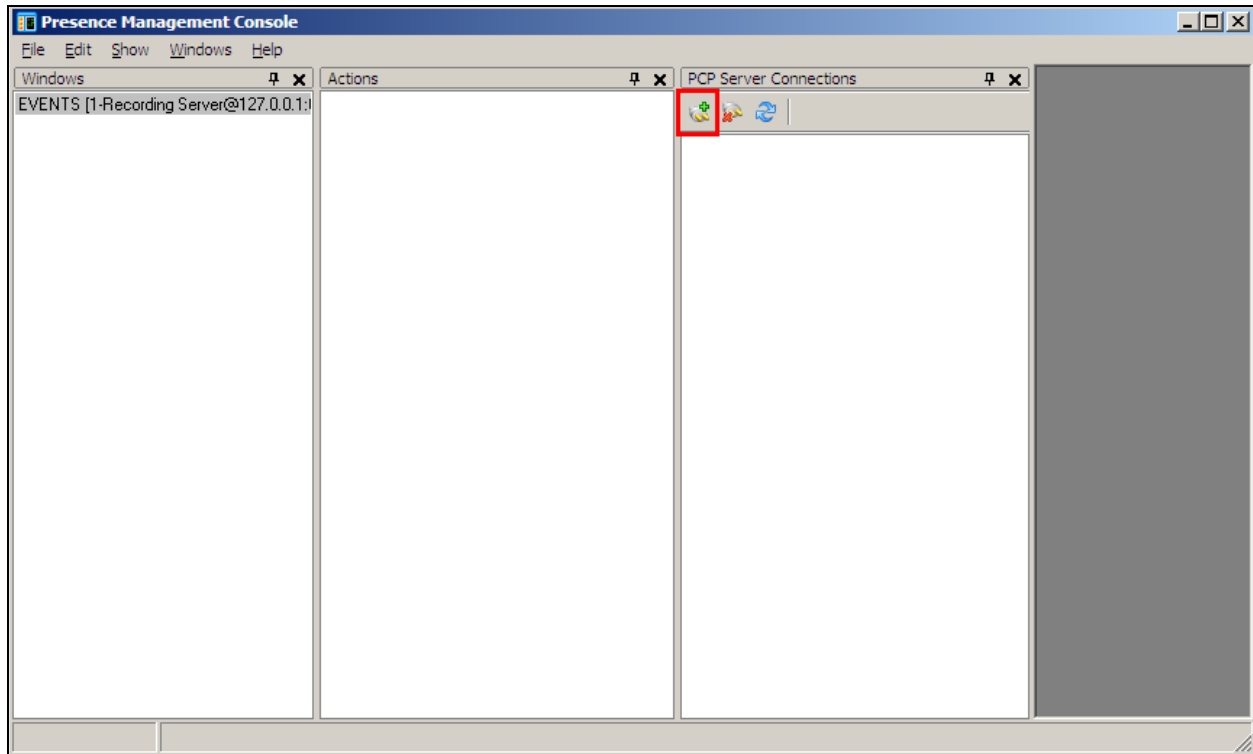
Calls that are placed via either of these Services will be recorded according to the recording plan configured above.



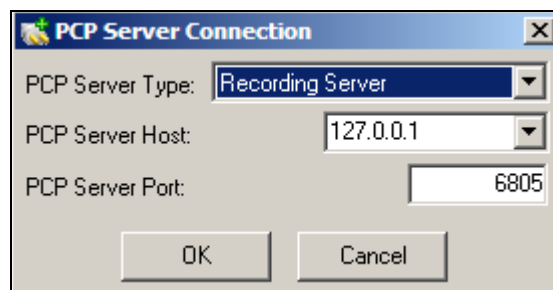
### 7.3. Add Avaya Aura® Communication Manager Stations to be Recorded

If the **Integrated with Presence Server** box is not ticked in Section 7.1 then each station that is to be recorded must be added. In the example below extensions 8270001 and 8270002 are added to be recorded by Presence Recording.

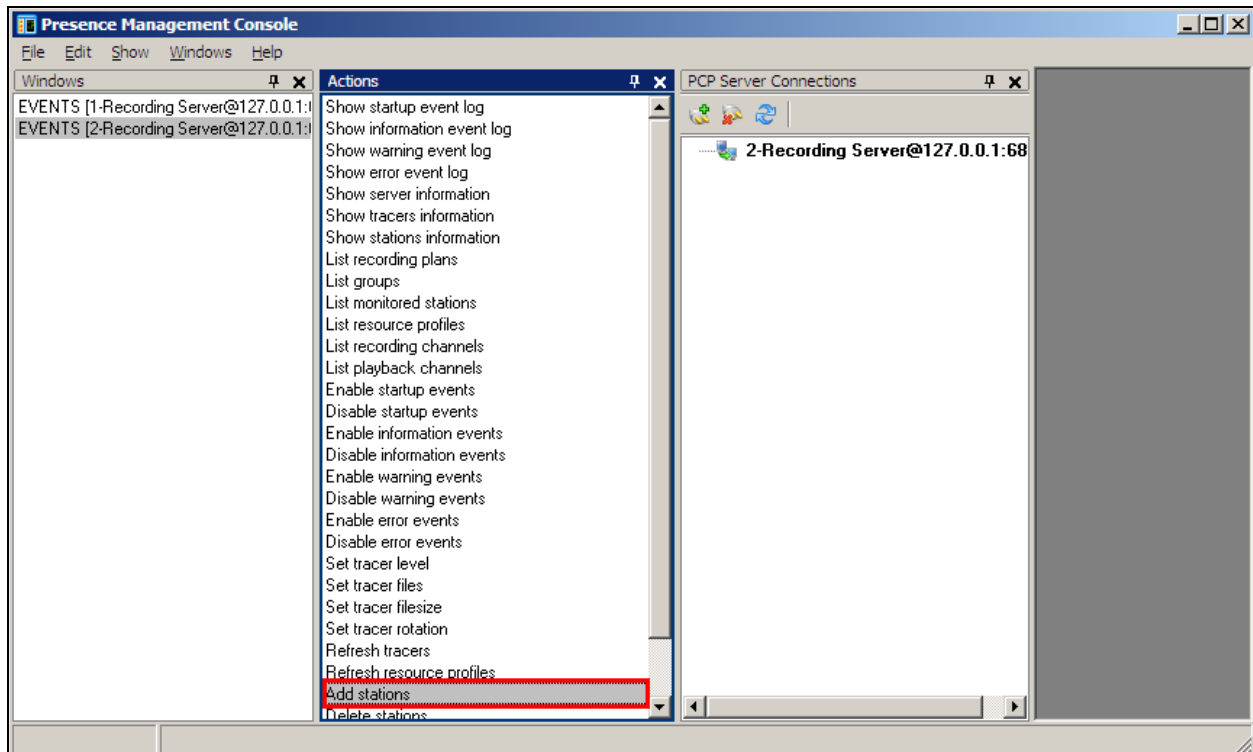
From the Presence folder, double-click on **pmconsole.exe** (not shown). The following window is opened, click on the connect icon as shown below.



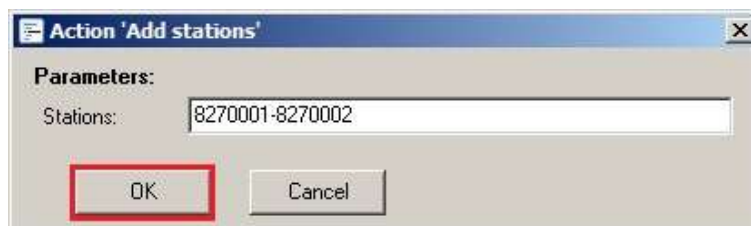
Select Recording Server from the drop down box **PCP Server Type**, ensure that the **Host** is set to the localhost **127.0.0.1** and the **Port** is set to **6805**.



From the middle window, select **Add Stations**.



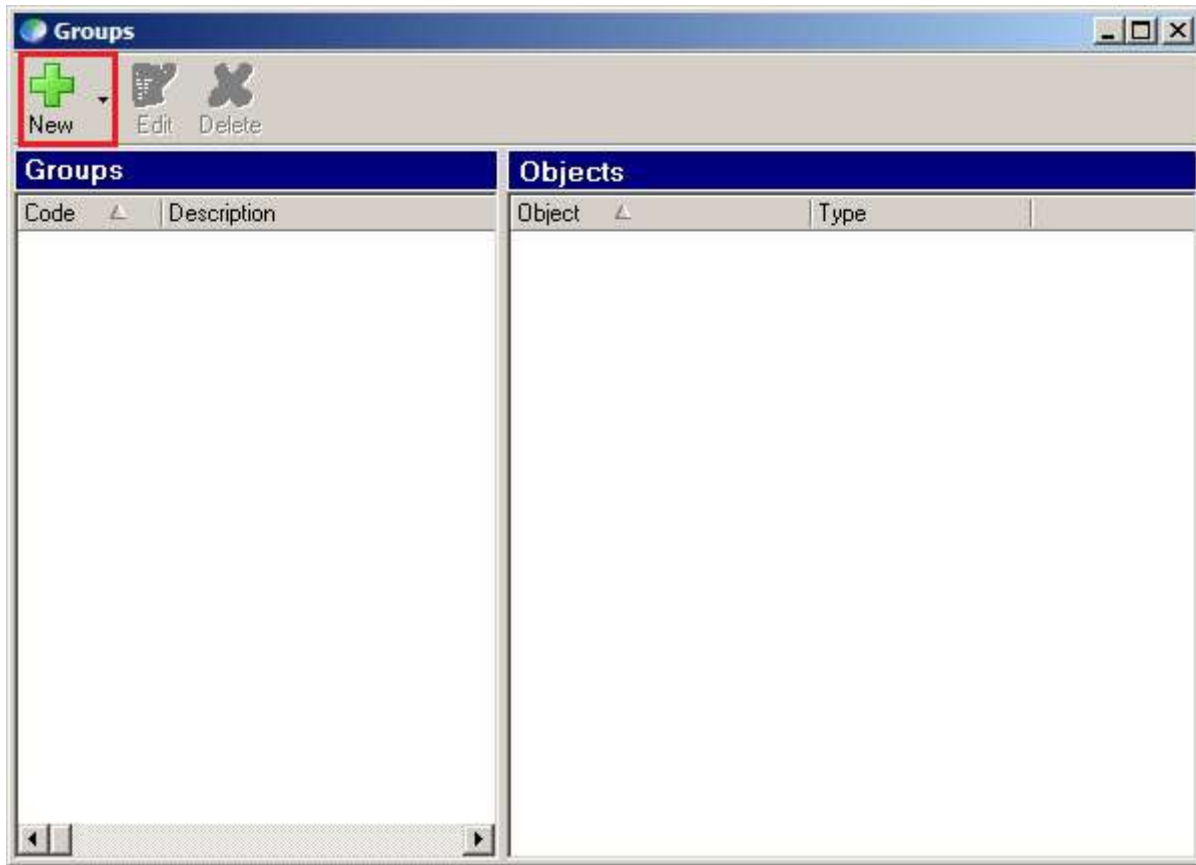
Enter the stations to be recorded and click **OK** when finished.



The following screen appears showing the stations are added.



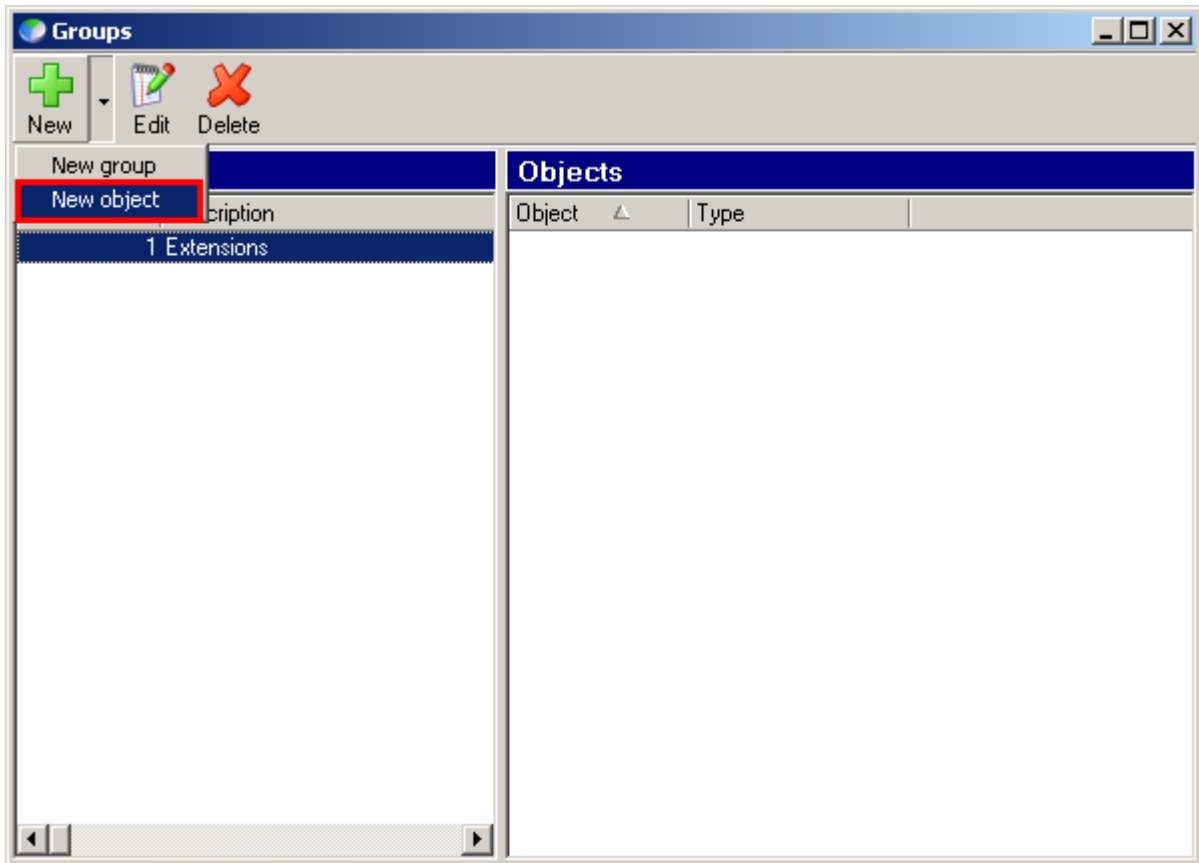
Open the Presence Recording Supervisor (precsup.exe) (not shown). Navigate to **Recordings→Groups** (not shown) and click on **New** in the window that appears.



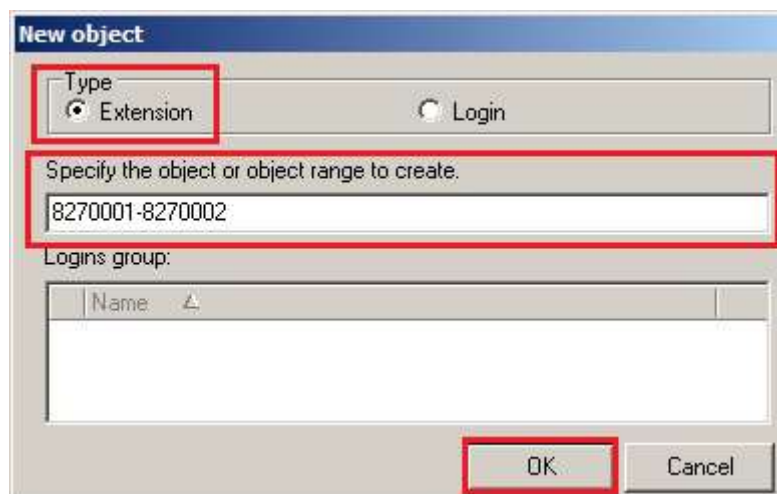
Enter the details for the new group. Note any number is used for code. Click on **OK** when finished.



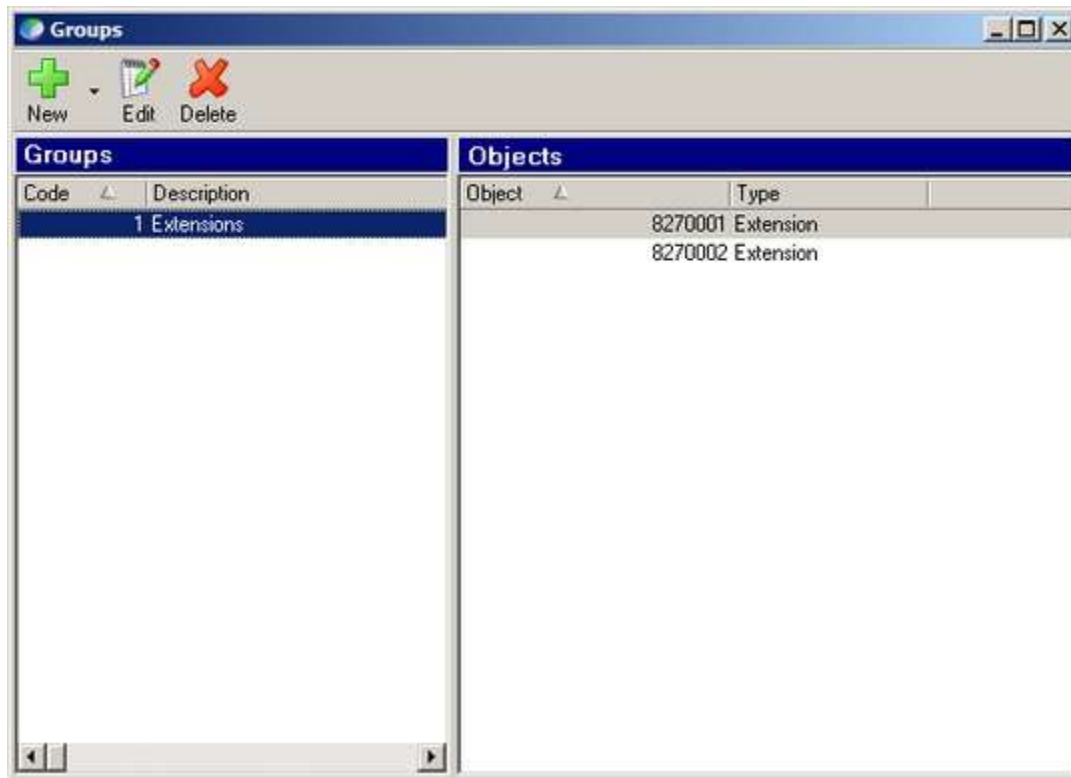
Click on **New** (drop-down box) and select **New object**.



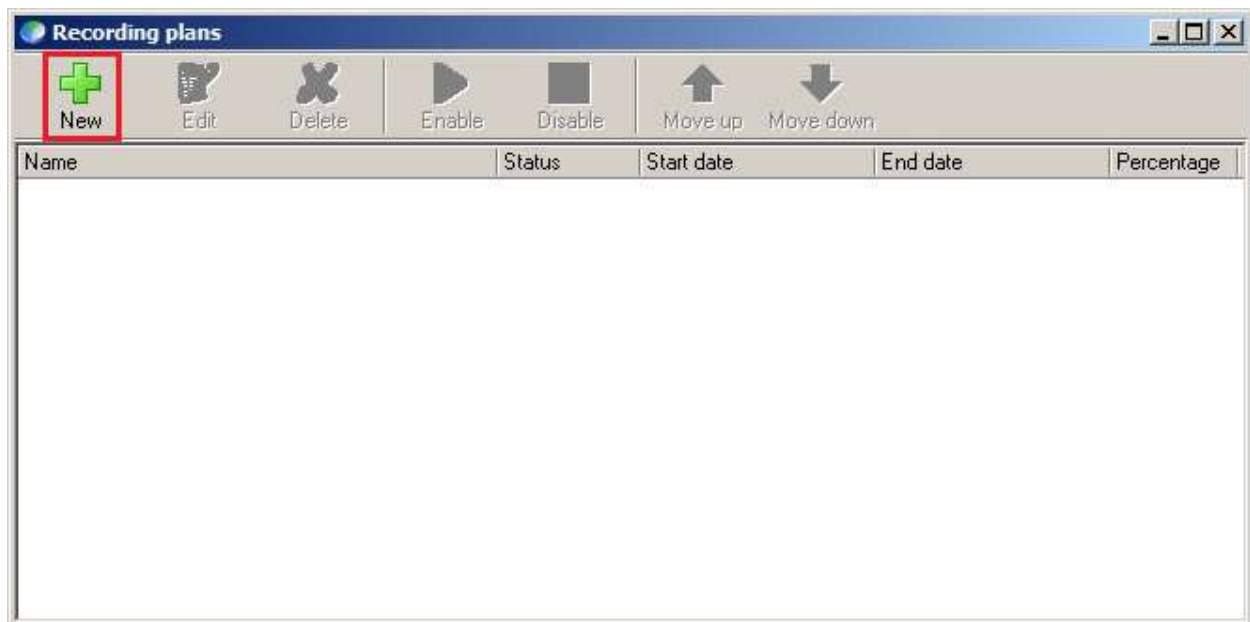
Select **Extension** as the **Type** and the extensions to be added. Click on **OK** once done.



Once **OK** is clicked above, the following screen shows the added stations.



Navigate to **Recordings**→**plans** (not shown) and click on **New** in the window that appears.



Enter a **Name**, the **Resource profile** is pre-selected, **Percentage to record** is set to **100%**. **Start** and **End** is set to **Immediately** and **Indeterminate** respectively. Click on **OK** once done.

The screenshot shows the 'New recording plan' dialog box with the 'General' tab selected. The left sidebar lists 'General', 'Screen recording', 'Services', and 'Groups'. The main area has a 'Name' field with 'Recording extensions', a 'Resource profile' dropdown set to 'General', and a 'Percentage to record' field set to '100 %'. Below these are 'Start' and 'End' sections, each with radio buttons for 'Immediately' and 'Date'. The 'Start' section has 'Immediately' selected, and the 'End' section has 'Indeterminate' selected. At the bottom are two unchecked checkboxes: 'Allow the agent to pause recordings' and 'Allow the agent to stop recordings'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

On the **Groups** window click on the Search icon on the right and select the group code to be recorded. Select the group created above (not shown) and click **OK**.

The screenshot shows the 'New recording plan' dialog box with the 'Groups' tab selected. The left sidebar lists 'General', 'Screen recording', 'Services', and 'Groups', with 'Groups' highlighted. The main area has a 'Group code' field. Below it are three icons: a green plus, a red X, and a magnifying glass (search icon) which is highlighted with a red rectangle. Below the icons is a table with two columns: 'Code' and 'Description'. The table is currently empty. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

## 8. Verification Steps

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

### 8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status with AES by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	AES71678	established	18	18

### 8.2. Verify TSAPI Link and DMCC

#### 8.2.1. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

The screenshot shows the AES Management Console interface. On the left is a sidebar with a navigation menu. The 'Status' section is expanded, and 'Status and Control' is selected. Under 'Status and Control', 'TSAPI Service Summary' is highlighted. The main content area displays the 'TSAPI Link Details' screen. At the top, there is a checkbox for 'Enable page refresh every 60 seconds'. Below this is a table with the following columns: Link, Switch Name, Switch CTI Link ID, Status, Since, and State. The table contains one row with the following data: Link 1, Switch Name CM1627, Switch CTI Link ID 1, Status Talking, Since Mon Nov 16 14:54:50 2015, and State Online. Below the table are two buttons: 'Online' and 'Offline'. At the bottom, there is a section titled 'For service-wide information, choose one of the following:' with three buttons: 'TSAPI Service Status', 'TLink Status', and 'User Status'.

### 8.2.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on AES to validate that the communication link between AES and the Presence Recording server is functioning correctly. Verify the status of the DMCC service by selecting **Status** → **Status and Control** → **DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to the Presence Recording server, IP address **10.10.16.127**. The **Application** is shown as **precserver.exe**, and the **Far-end Identifier** is given as the IP address **10.10.16.127** as expected. The **User** is shown as the user created for the CTI user for Presence Server, in this case **Presenceco**.

The screenshot shows the 'DMCC Service Summary - Session Summary' page. On the left is a navigation menu with categories like 'All Services', 'Communication Manager', 'Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', and 'Status'. Under 'Status', there are links for 'Alarm Viewer', 'Log Manager', 'Logs', and 'Status and Control'. The 'Status and Control' section is expanded, showing links for 'CVLAN Service Summary', 'DLG Services Summary', 'DMCC Service Summary' (which is selected), and 'Switch Conn Summary'.

The main content area is titled 'DMCC Service Summary - Session Summary'. It includes a warning 'Please do not use back button' and a checkbox for 'Enable page refresh every 60 seconds'. Below this, it shows 'Session Summary' and 'Device Summary' links. The session was generated on 'Wed Nov 18 12:01:55 GMT 2015'. It lists 'Service Uptime: 2 days, 0 hours 29 minutes', 'Number of Active Sessions: 1', 'Number of Sessions Created Since Service Boot: 24', 'Number of Existing Devices: 6', and 'Number of Devices Created Since Service Boot: 130'.

A table displays session details:

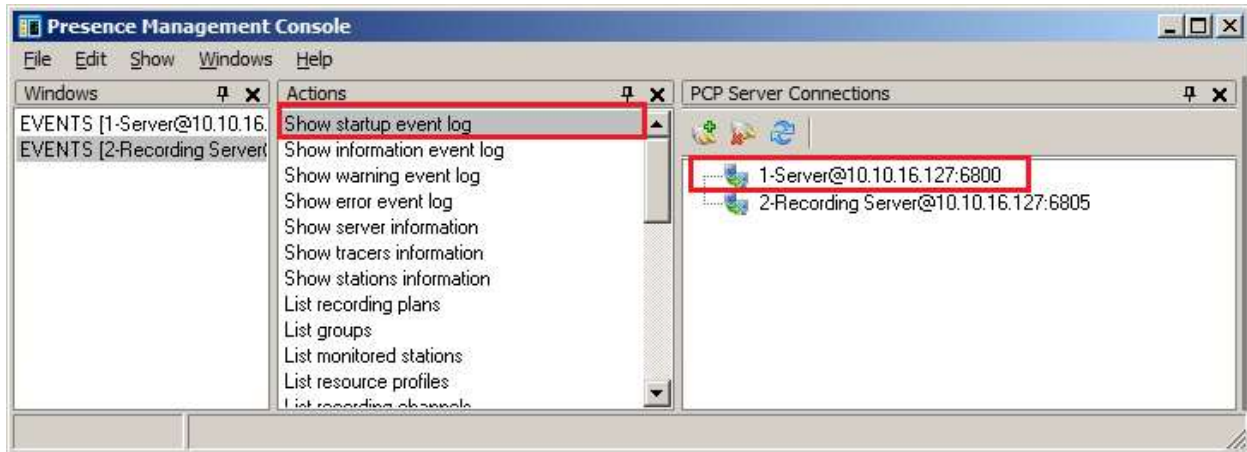
	Session ID	User	Application	Far-end Identifier	Connection Type	#
<input type="checkbox"/>	0263C4551F2048F21 8E091B17A5533FA-27	presence	precserver.exe	10.10.16.127	XML Unencrypted	6

Below the table are buttons for 'Terminate Sessions' and 'Show Terminated Sessions'. At the bottom, it shows 'Item 1-1 of 1' and a 'Go' button.

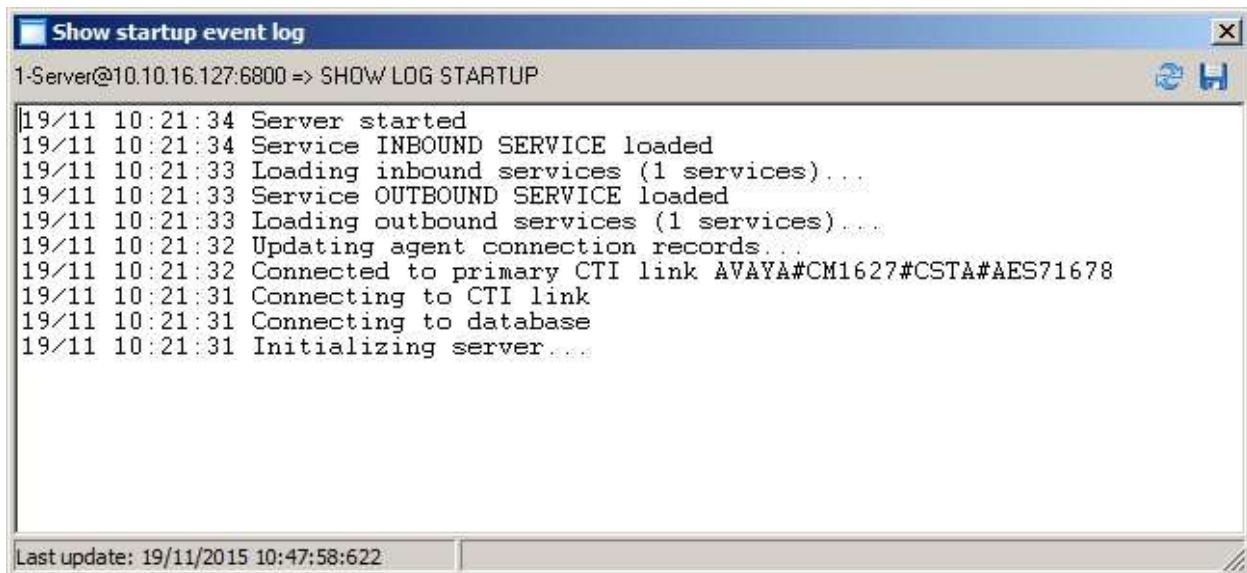


### 8.3. Verify Presence Suite CTI Connection

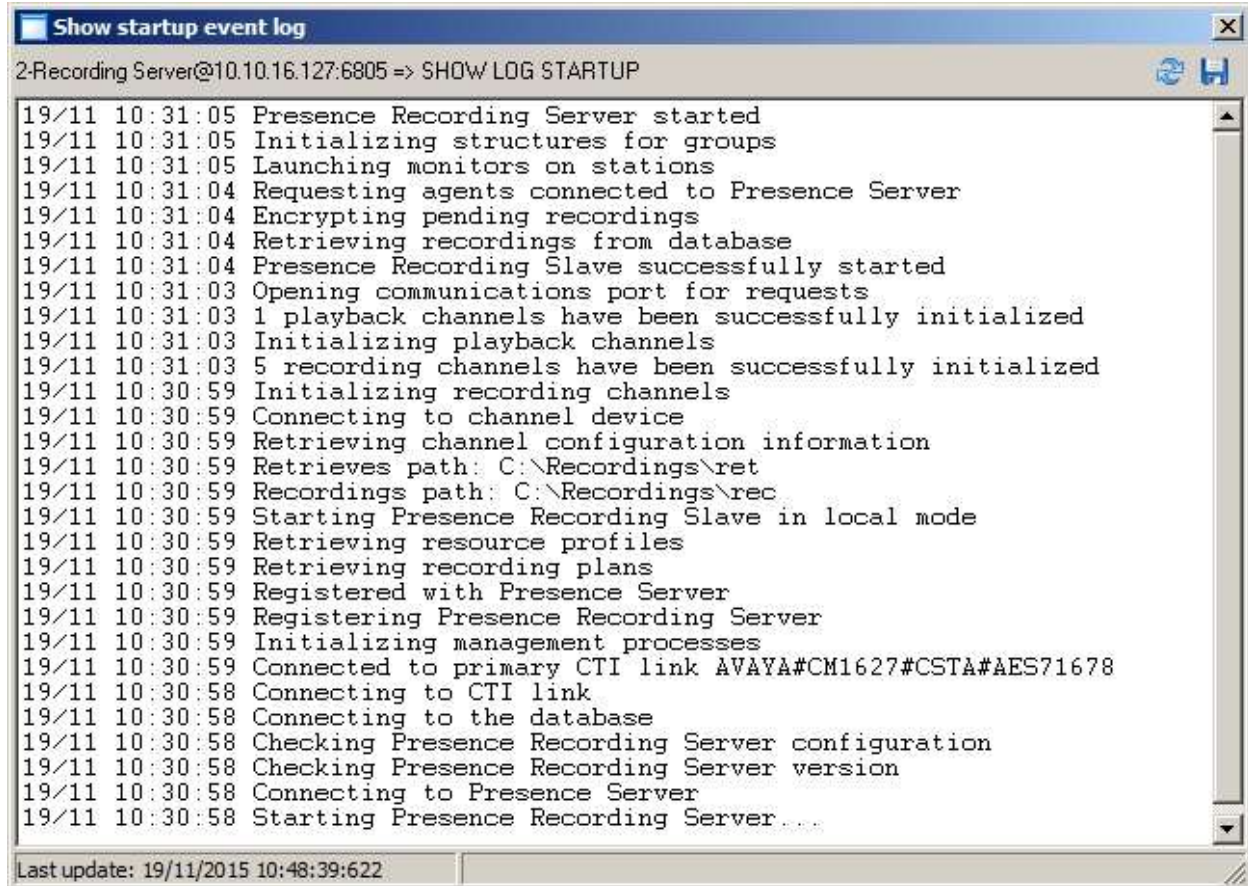
One of the available methods to confirm correct startup is a startup log which can be accessed from Presence Management Console. Navigate to **C: → Presence → pmconsole.exe** (not shown). A startup log commences when the Presence Server is trying to load and connect to AES. Click on the item named **Server@127.0.0.1:6800** in the **PCP Server Connections** pane of the Management Console. To open the startup event log, double click **Show startup event log** in the **Actions** pane.



Verify successful CTI connection and service startup.



Repeat the above for the item named **Recording Server@127.0.0.1:6805**.

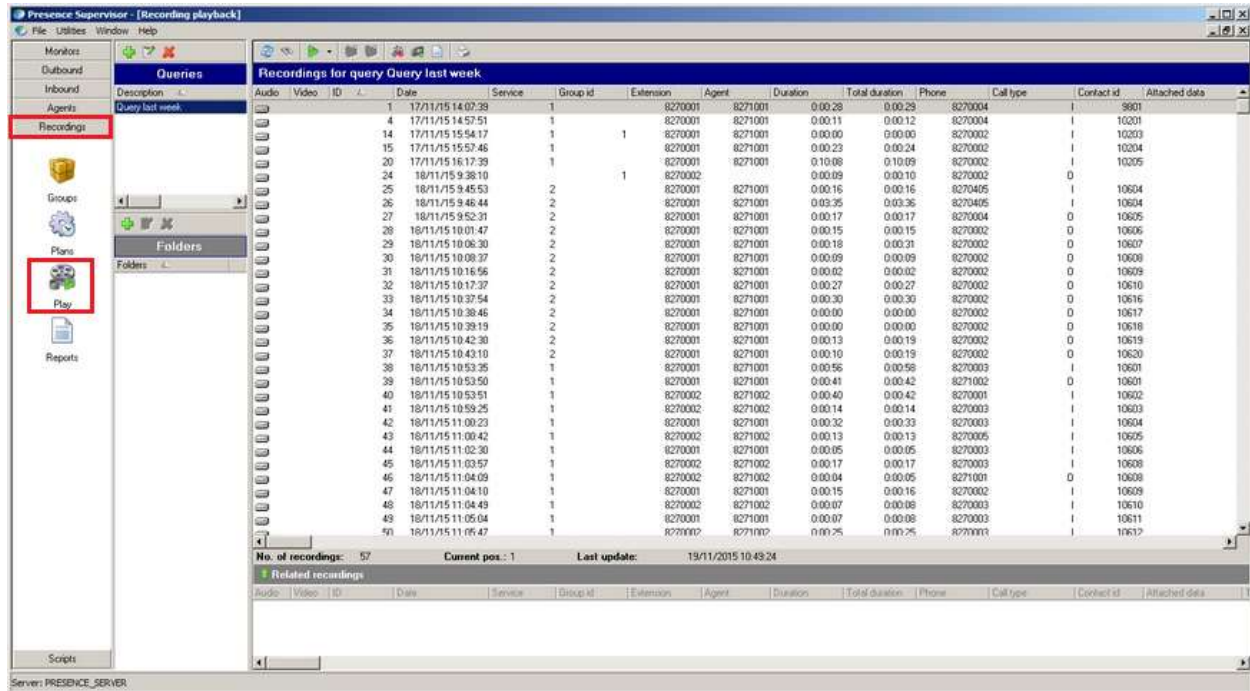


```
19/11 10:31:05 Presence Recording Server started
19/11 10:31:05 Initializing structures for groups
19/11 10:31:05 Launching monitors on stations
19/11 10:31:04 Requesting agents connected to Presence Server
19/11 10:31:04 Encrypting pending recordings
19/11 10:31:04 Retrieving recordings from database
19/11 10:31:04 Presence Recording Slave successfully started
19/11 10:31:03 Opening communications port for requests
19/11 10:31:03 1 playback channels have been successfully initialized
19/11 10:31:03 Initializing playback channels
19/11 10:31:03 5 recording channels have been successfully initialized
19/11 10:30:59 Initializing recording channels
19/11 10:30:59 Connecting to channel device
19/11 10:30:59 Retrieving channel configuration information
19/11 10:30:59 Retrieves path: C:\Recordings\ret
19/11 10:30:59 Recordings path: C:\Recordings\rec
19/11 10:30:59 Starting Presence Recording Slave in local mode
19/11 10:30:59 Retrieving resource profiles
19/11 10:30:59 Retrieving recording plans
19/11 10:30:59 Registered with Presence Server
19/11 10:30:59 Registering Presence Recording Server
19/11 10:30:59 Initializing management processes
19/11 10:30:59 Connected to primary CTI link AVAYA#CM1627#CSTA#AES71678
19/11 10:30:58 Connecting to CTI link
19/11 10:30:58 Connecting to the database
19/11 10:30:58 Checking Presence Recording Server configuration
19/11 10:30:58 Checking Presence Recording Server version
19/11 10:30:58 Connecting to Presence Server
19/11 10:30:58 Starting Presence Recording Server...
```

Last update: 19/11/2015 10:48:39:622

## 8.4. Verify Presence Recording Capture and Playback

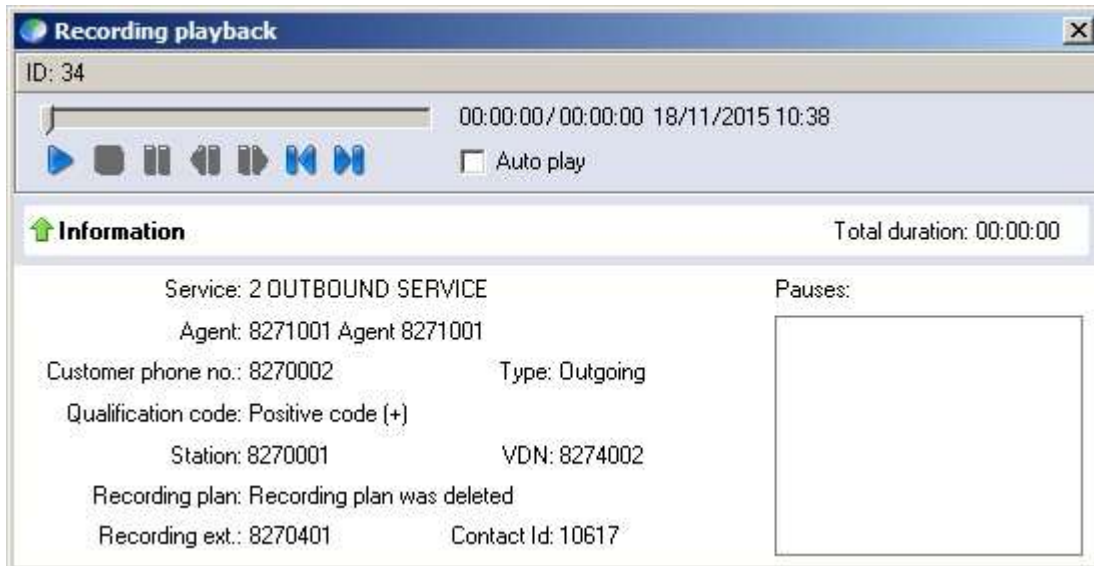
Using Presence Supervisor, click **Recordings** → **Play**, visually verify correct recording detail as shown below.



Double click on the recording to be played, the pop up shown below will be displayed with the prompt to dial a playback extension.



Dial the number shown and manually confirm accurate, clear and audible call recording playback. The screen below will be displayed allowing playback control.



## 9. Conclusion

These Application Notes describe the configuration steps required for Presence Technology Presence Recording R10.1 to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2**.

## 10. Additional References

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

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

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 7.0*

The following documentation is available on request from Presence: [www.presenceco.com](http://www.presenceco.com)

- [4] *ACD Sys Presence Administrator Manual Presence Suite*, V10.1
- [5] *Presence Installation Guides Presence Software*, V10.1
- [6] *PBX/ACD Requirements Presence Software*, V10.1

---

**©2015 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).