Application Notes for Presence Technology Presence Recording R11.0 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 - 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 R11.0 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1.

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 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Presence Recording did not include use of any specific encryption features as requested by Presence Technology.

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:

- Inbound ACD Calls
- Call Hold/Transfer/Conference
- Outbound Calls
- Inbound Calls (Recording on Demand)
- Outbound Calls (Recording on Demand)
- Serviceability Testing

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
Website:	www.presenceco.com
Phone:	+34 93 10 10 300

3. Reference Configuration

Figure 1 shows the network topology during interoperability testing. 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.

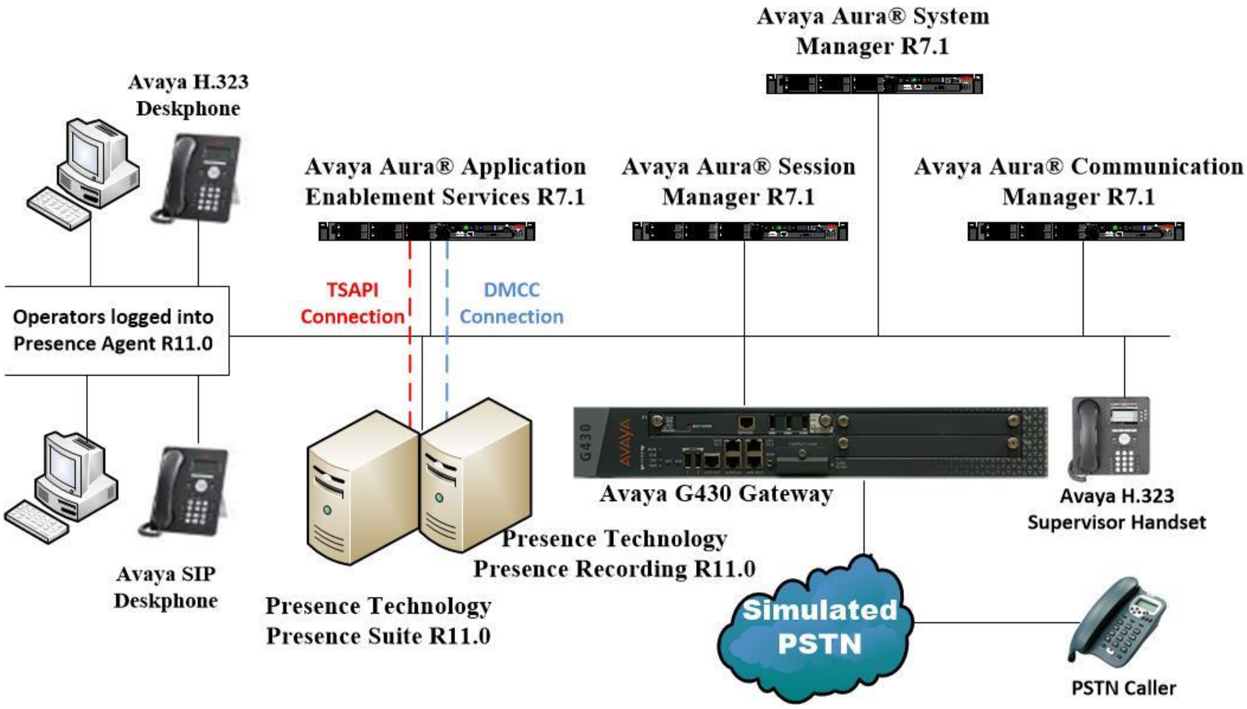

Avaya Aura® System Manager R7.1
Avaya H.323 Deskphone
Avaya Aura® Application Enablement Services R7.1
Avaya Aura® Session Manager R7.1
Avaya Aura® Communication Manager R7.1
TSAPI Connection
DMCC Connection
Operators logged into Presence Agent R11.0
Avaya G430 Gateway
Avaya H.323 Supervisor Handset
Presence Technology Presence Recording R11.0
Avaya SIP Deskphone
Presence Technology Presence Suite R11.0
Simulated PSTN
PSTN Caller

Figure 1: Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 with Presence Technology Presence Suite Server with Presence Recording R11.0 configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.1.1.0 Build No. - 7.1.0.0.1125193 Software Update Revision No: 7.1.1.0.046931 Feature Pack 1 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.1 SP1 Build No. – 7.1.1.0.711008
Avaya Aura® Communication Manager running on virtual server	R017x.01.0.532.0 R7.1.1.0.0 - FP1 Update ID 01.0.532.0-23985
Avaya Aura® Application Enablement Services	R7.1
Avaya Aura® Media Server running on virtual server	R7.8
Avaya G430 Gateway	37.42.0 /1
Avaya 96x1 H323 Deskphone	96x1 H323 Release 6.6401
Avaya 96x1 SIP Deskphone	96x1 SIP Release 7.1.0.1.1
Presence Technology Presence Suite running on Windows Server 2016	R11.0
Presence Technology Presence Recording running on Windows Server 2016	R11.0
Presence Technology Presence Client running on Windows 7 SP1	R11.0

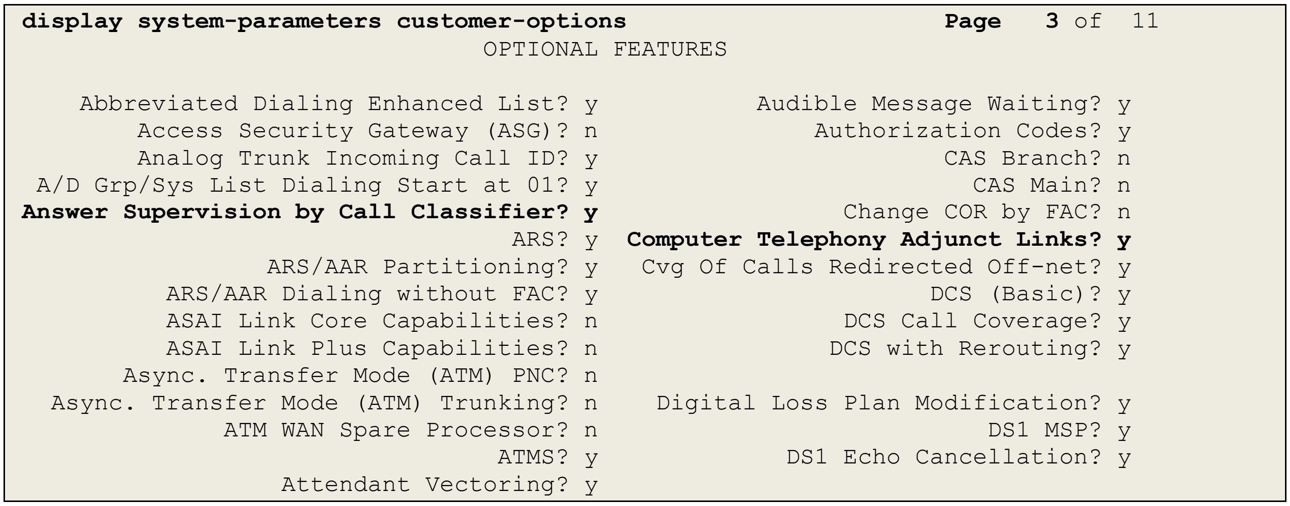
5. Configure Avaya Aura® Communication Manager

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 R11.0 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1.*

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
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

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 (**AES71vmpg**).

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
AES71vmpg           10.10.40.43
AMS71vmpg           10.10.40.49
GW71vmpg            10.10.40.15
SM70vmpg            10.10.40.12
SM71vmpg            10.10.40.52
default             0.0.0.0
procr               10.10.40.47
procr6              ::
```

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 5.2**.
- **Local Port** Retain the default value of **8765**.

```
change ip-services                                                Page   1 of   4

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

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 **AES71vmpg**.
- **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       Password          Enabled    Status
                   Server
      1:        AES71vmpg         ********          y          idle
      2:
      3:
```

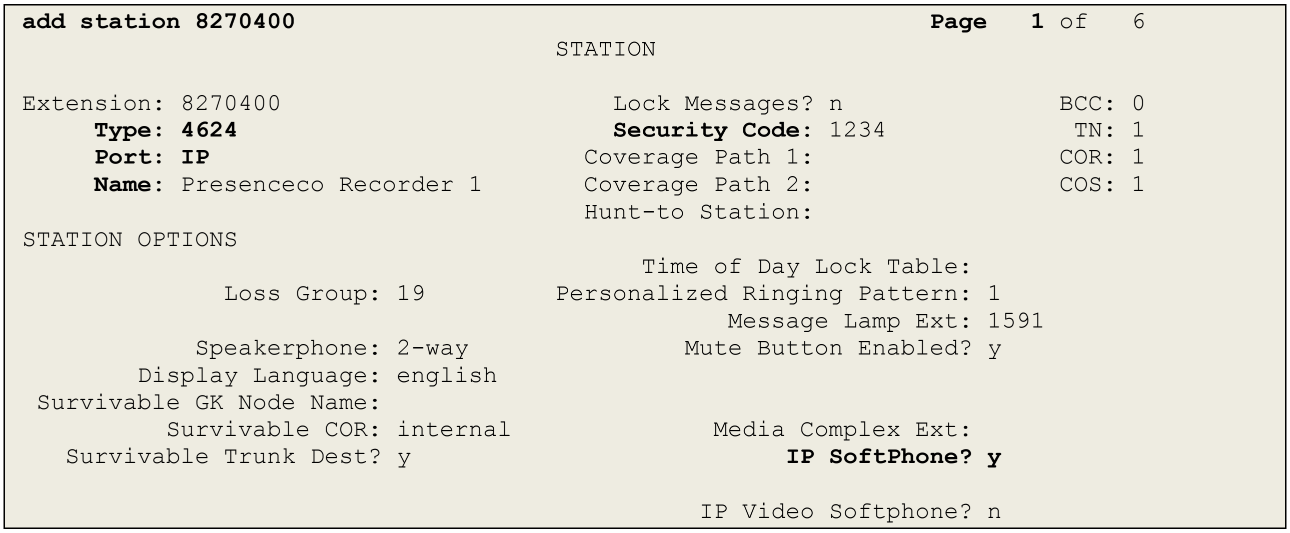
5.4. Configure CTI Link for TSAPI Service

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: 4499
     Type: ADJ-IP
                                                                          COR: 1
     Name: AES71vmpg
```

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
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 1591
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                               IP Video Softphone? n
```

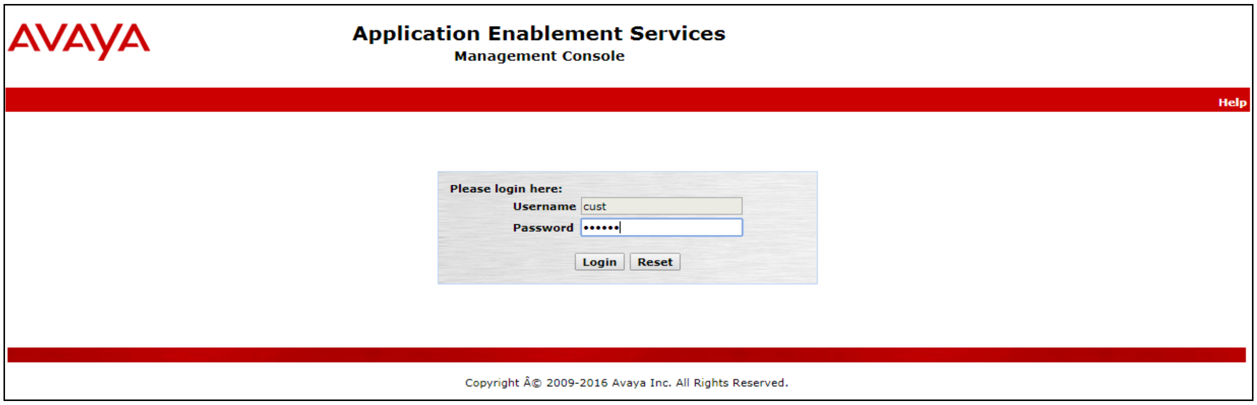
6. Configure Avaya Aura® Application Enablement Services

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
- Enable DMCC Ports

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.



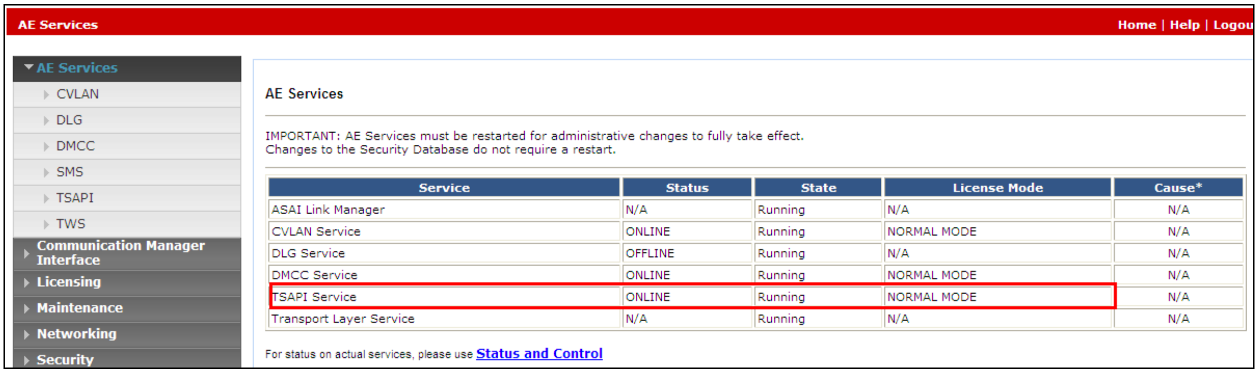
Please login here:

Username cust

Password ••••••

Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

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.



AE Services

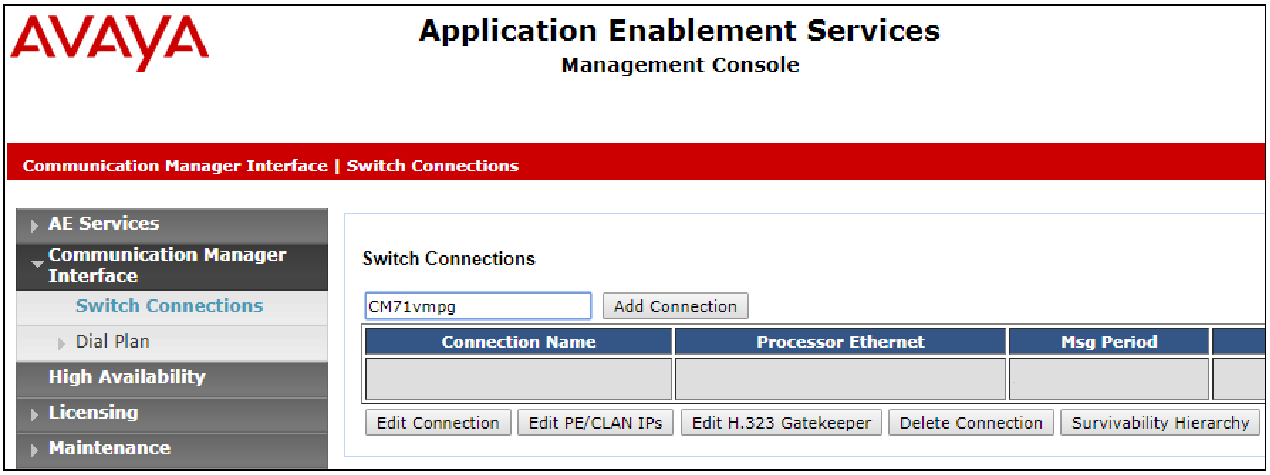
IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

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

For status on actual services, please use Status and Control

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.


AVAYA
Application Enablement Services
Management Console
Communication Manager Interface | Switch Connections
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance

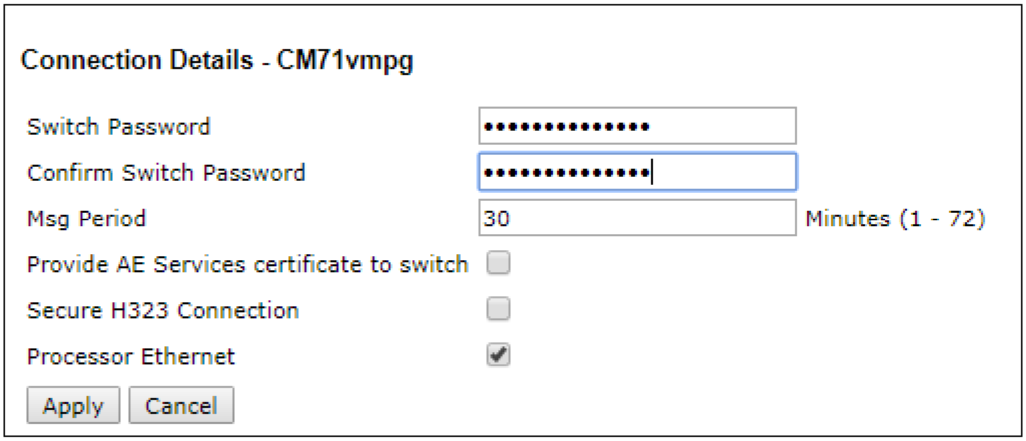
Switch Connections

CM71vmpg [Add Connection]

Connection Name	Processor Ethernet	Msg Period

[Edit Connection] [Edit PE/CLAN IPs] [Edit H.323 Gatekeeper] [Delete Connection] [Survivability Hierarchy]

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 5.3**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

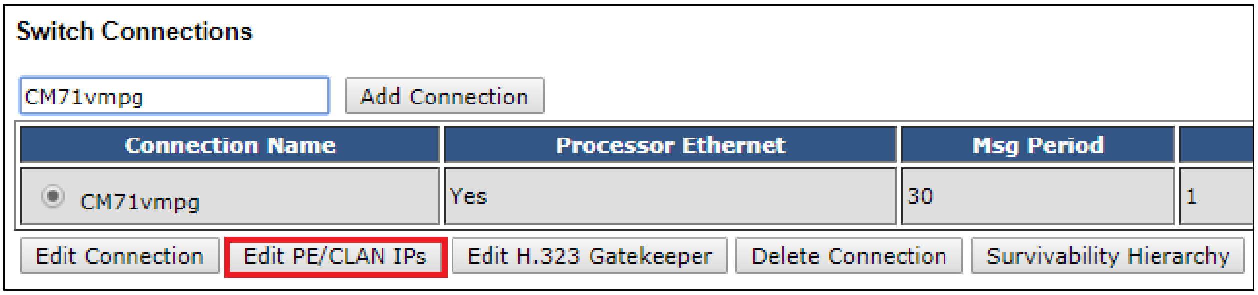


Connection Details - CM71vmpg

Switch Password	••••••••••••••	
Confirm Switch Password	••••••••••••••	
Msg Period	30	Minutes (1 - 72)
Provide AE Services certificate to switch	☐	
Secure H323 Connection	☐	
Processor Ethernet	☑	

[Apply] [Cancel]

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown).

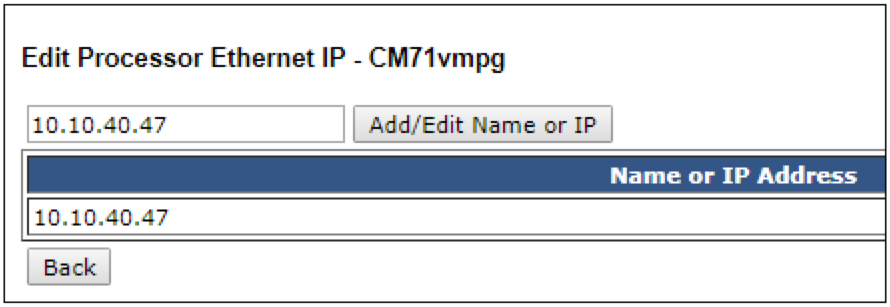


Switch Connections

CM71vmpg

Connection Name	Processor Ethernet	Msg Period	
● CM71vmpg	Yes	30	1

In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.2** that will be used for the AES connection and select the **Add Name or IP** button.



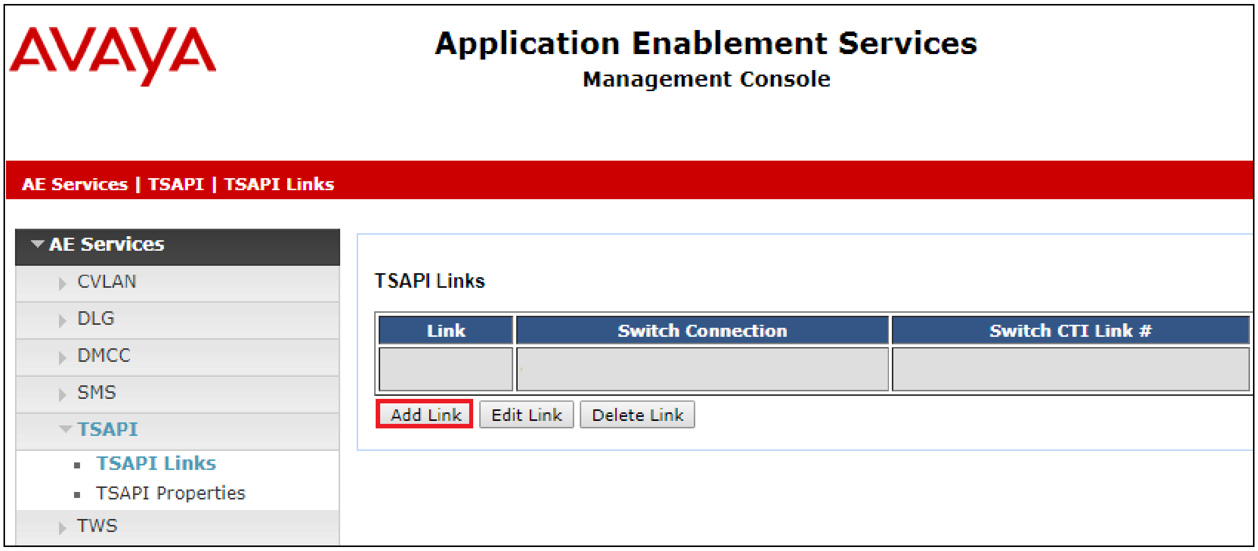
Edit Processor Ethernet IP - CM71vmpg

10.10.40.47

Name or IP Address
10.10.40.47

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.

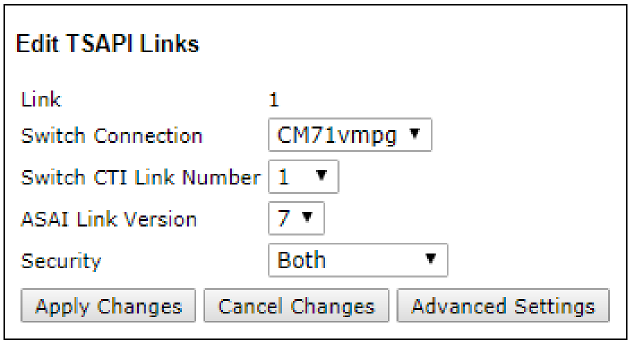


TSAPI Links

Link	Switch Connection	Switch CTI Link #

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

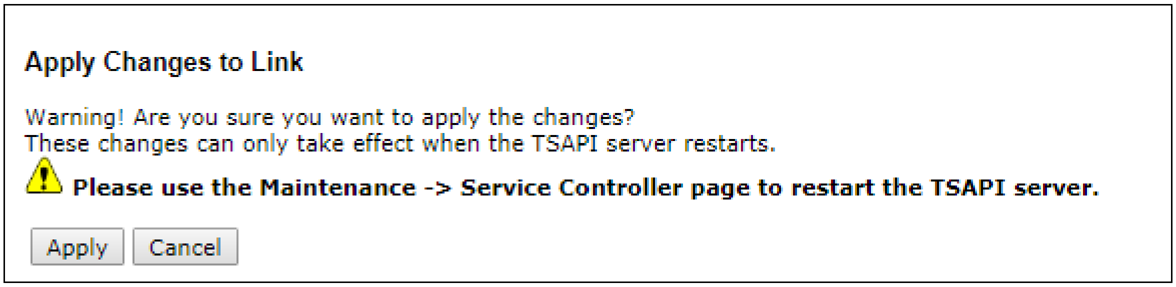
- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM71vmpg**, which has already been configured in **Section 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.3**.
- **ASAI Link Version:** This can be left at the default value of **7**.
- **Security:** This can be left at the default value. The value **both** was used in this test.
- Once completed, select **Apply Changes**.



Edit TSAPI Links

Link	1
Switch Connection	CM71vmpg ▼
Switch CTI Link Number	1 ▼
ASAI Link Version	7 ▼
Security	Both ▼

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

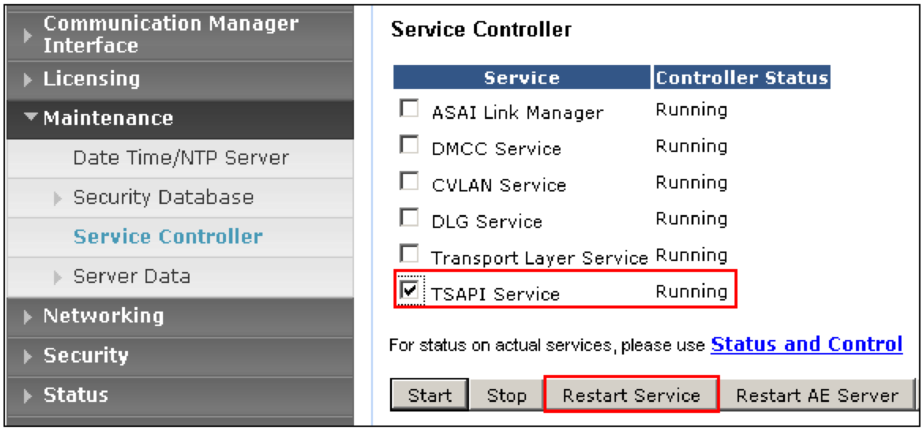


Apply Changes to Link

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**.



Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

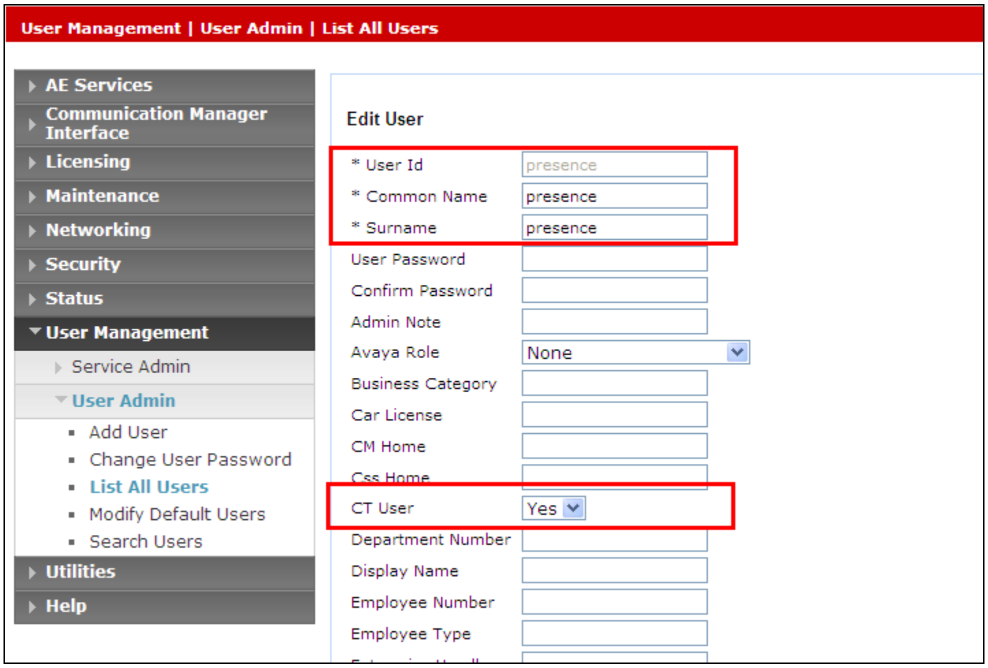
For status on actual services, please use Status and Control

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).



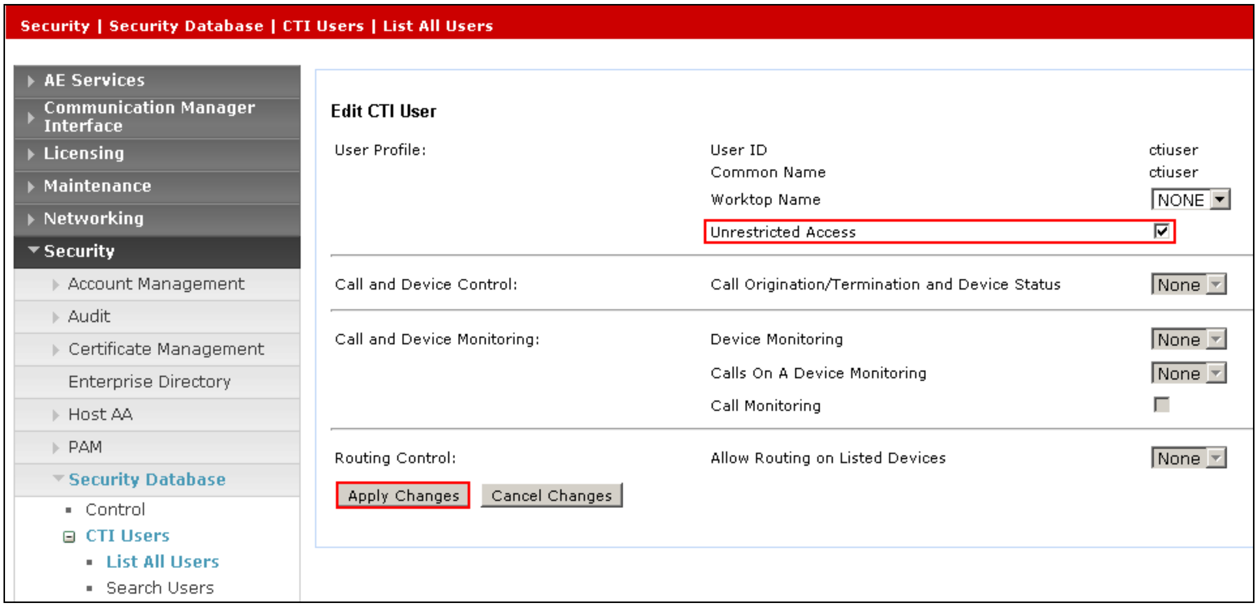
Edit User

* User Id	presence
* Common Name	presence
* Surname	presence
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	

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.



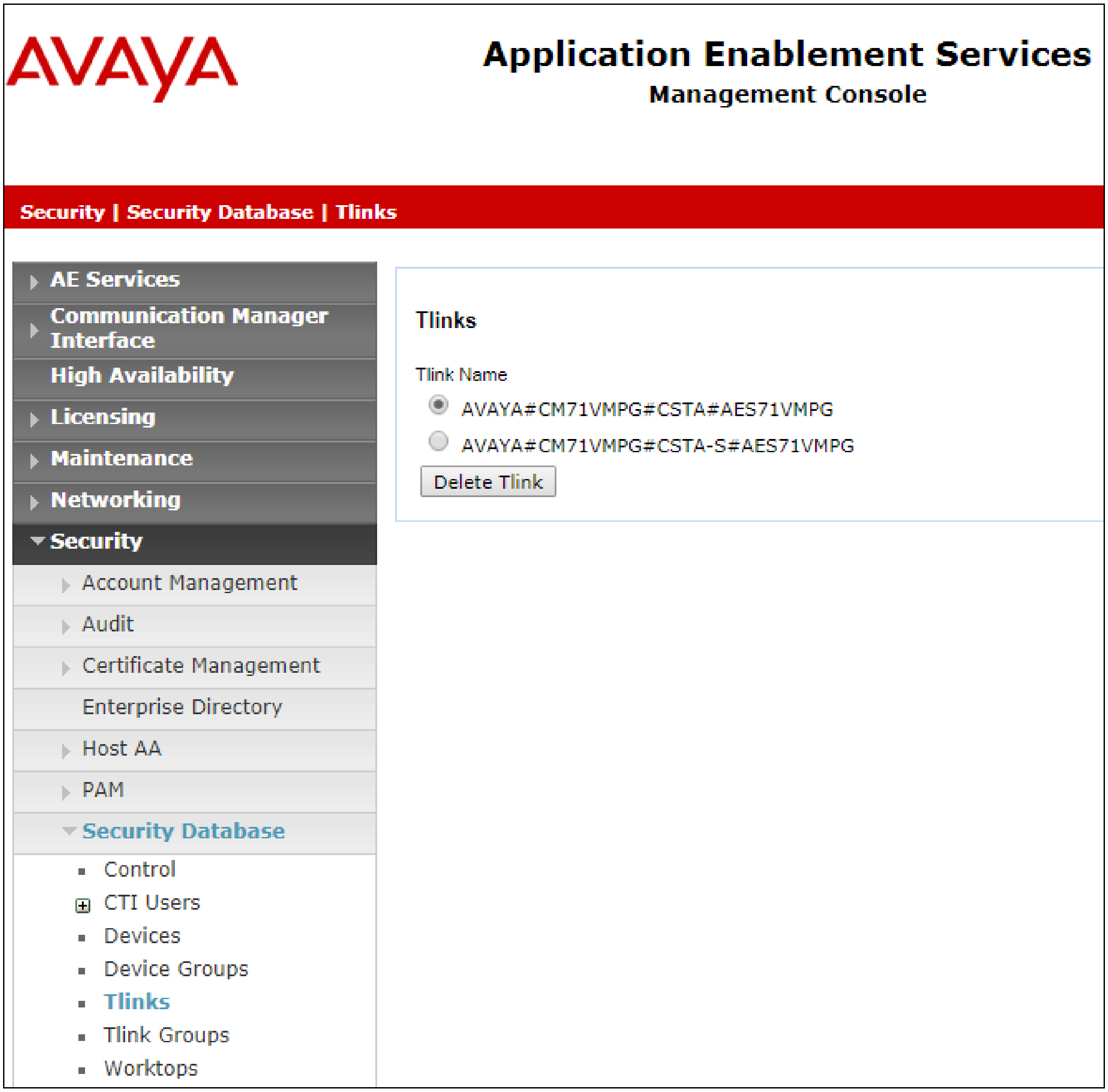
Edit CTI User

User Profile:	User ID	ctiuser
	Common Name	ctiuser
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

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**.



Tlinks

Tlink Name

● AVAYA#CM71VMPG#CSTA#AES71VMPG

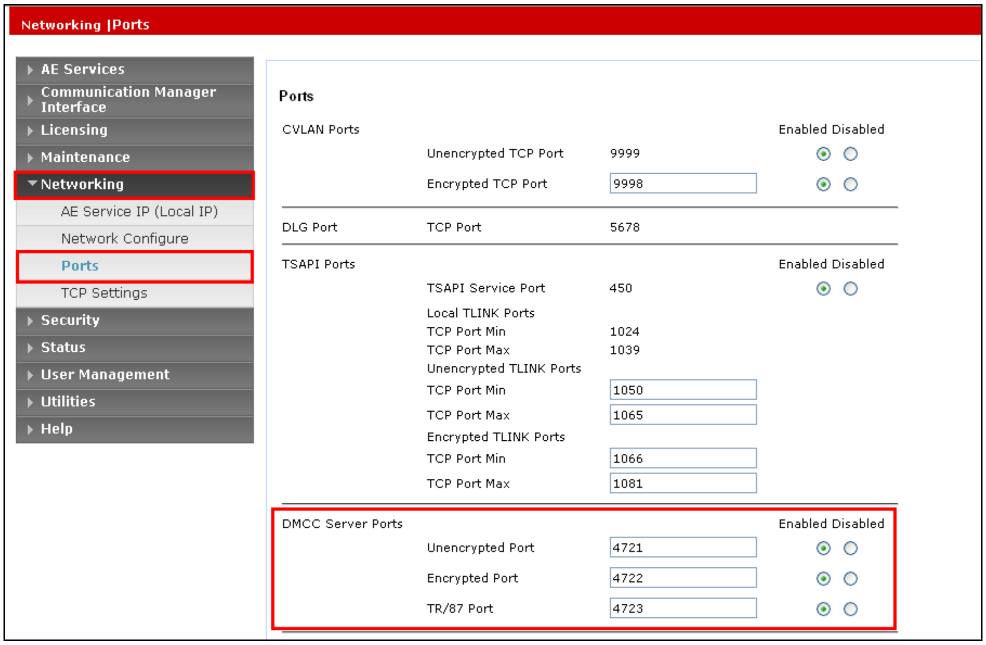
○ AVAYA#CM71VMPG#CSTA-S#AES71VMPG

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**

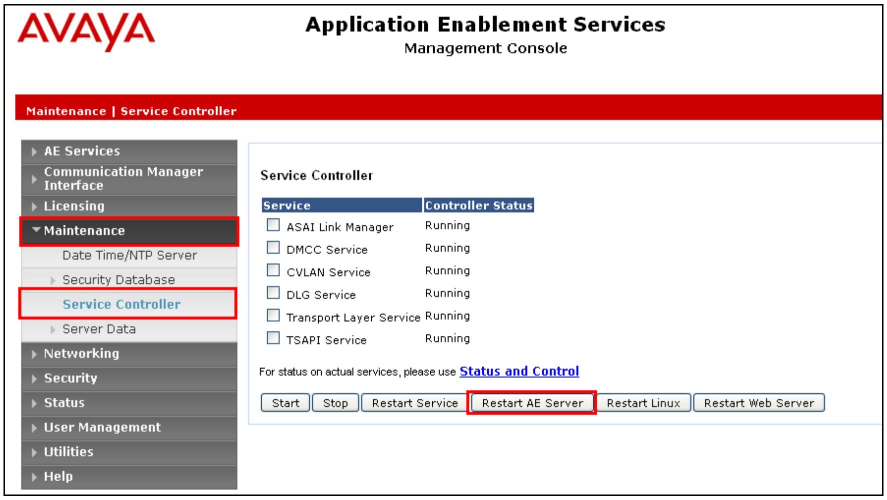
Click on **Apply Changes** at the bottom of the screen (not shown).



Ports

CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

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.



Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
□ TSAPI Service	Running

For status on actual services, please use Status and Control

7. Configure Presence Recording

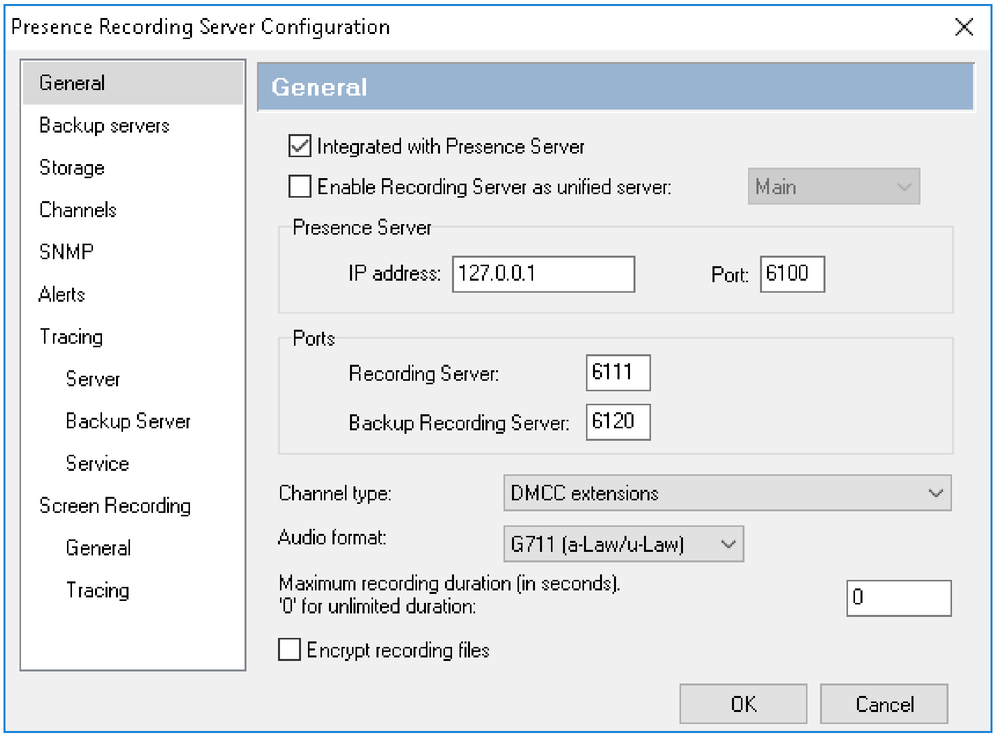
The Presence Recording can be an additional component of Presence Suite but may also be installed as a stand-alone product. These Application Notes will show the configuration for both instances in both cases the Presence Recording Server must be configured to connect with AES.

The Presence Suite includes the Presence Server, Presence Mail Interactions Server, Presence Web Interactions Server, Presence Administrator, Presence Web 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 R11.0 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1*.

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 Sever 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.



Presence Recording Server Configuration

General

☑ Integrated with Presence Server

☐ Enable Recording Server as unified server: Main

Presence Server

IP address: 127.0.0.1 Port: 6100

Ports

Recording Server: 6111

Backup Recording Server: 6120

Channel type: DMCC extensions

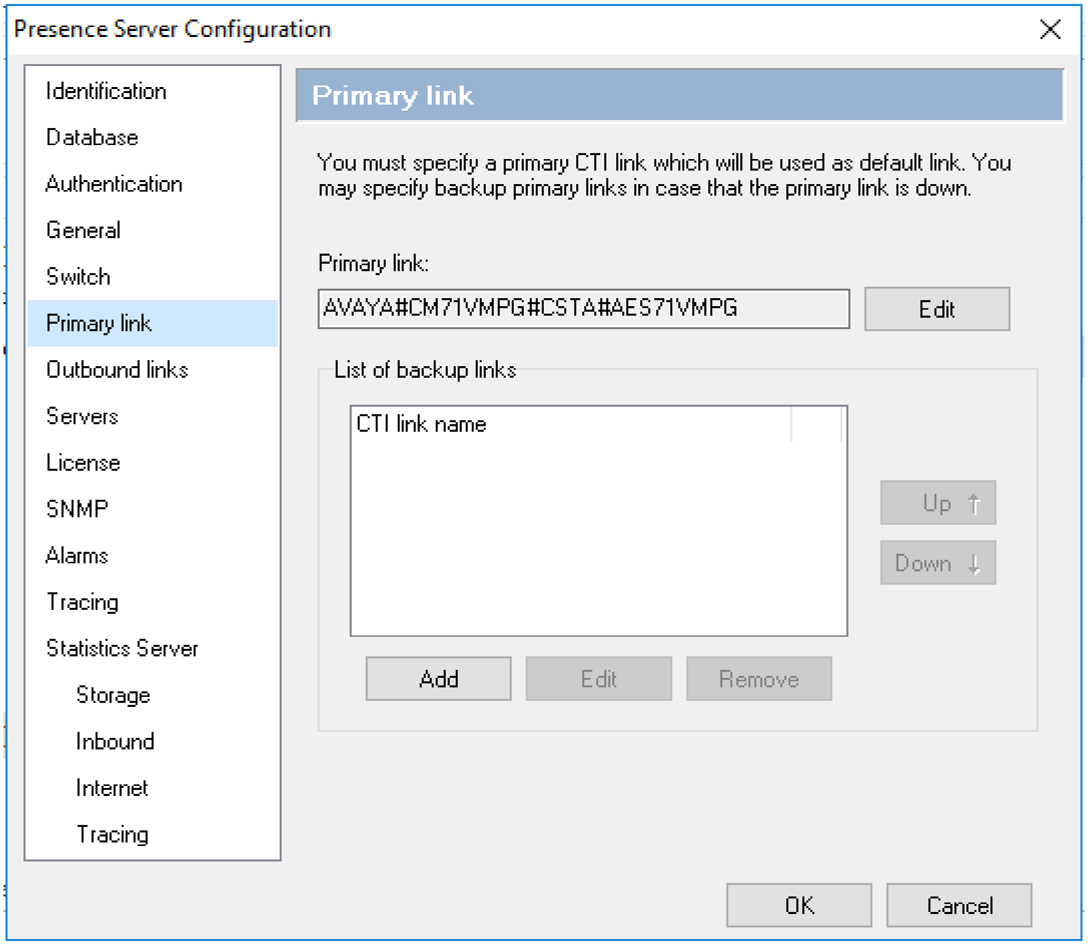
Audio format: G711 (a-Law/u-Law)

Maximum recording duration (in seconds). '0' for unlimited duration: 0

☐ Encrypt recording files

7.1.1. Configure the CTI Connection

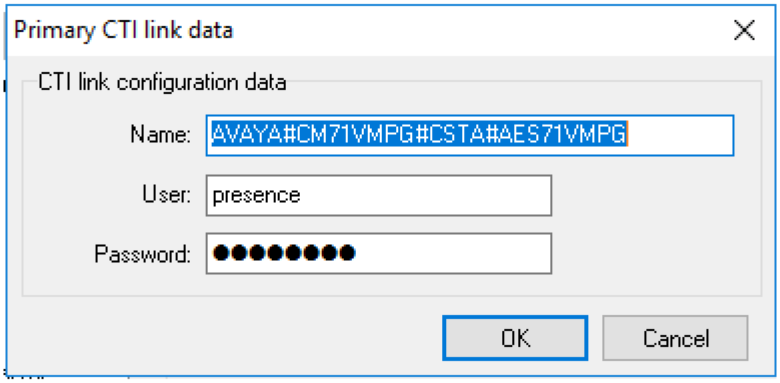
If the CTI connection is not in place select the **Primary link** menu on the left side of the screen and choose the **Edit** button to enter a value.



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.

Primary link: AVAYA#CM71VMPG#CSTA#AES71VMPG

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**.



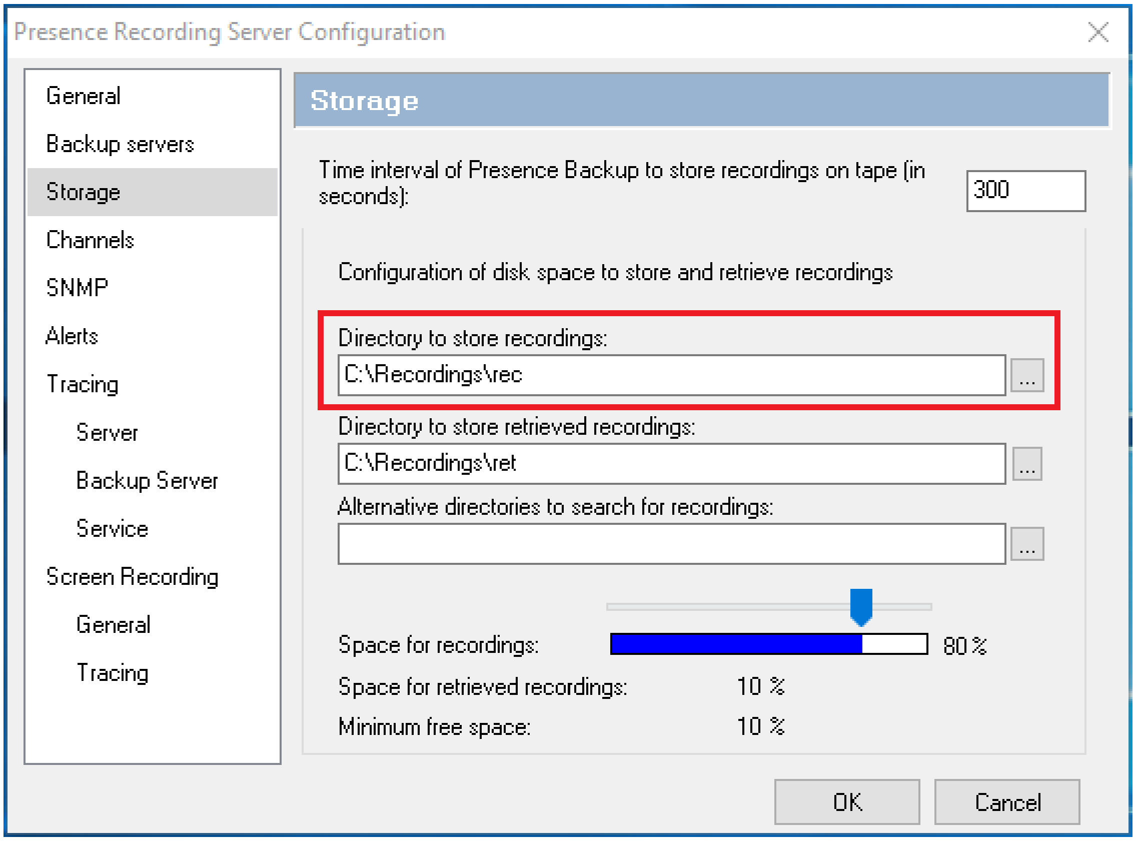
Name: AVAYA#CM71VMPG#CSTA#AES71VMPG

User: presence

Password: ●●●●●●●●

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.



Time interval of Presence Backup to store recordings on tape (in seconds): 300

Configuration of disk space to store and retrieve recordings

Directory to store recordings: C:\Recordings\rec

Directory to store retrieved recordings: C:\Recordings\ret

Alternative directories to search for recordings:

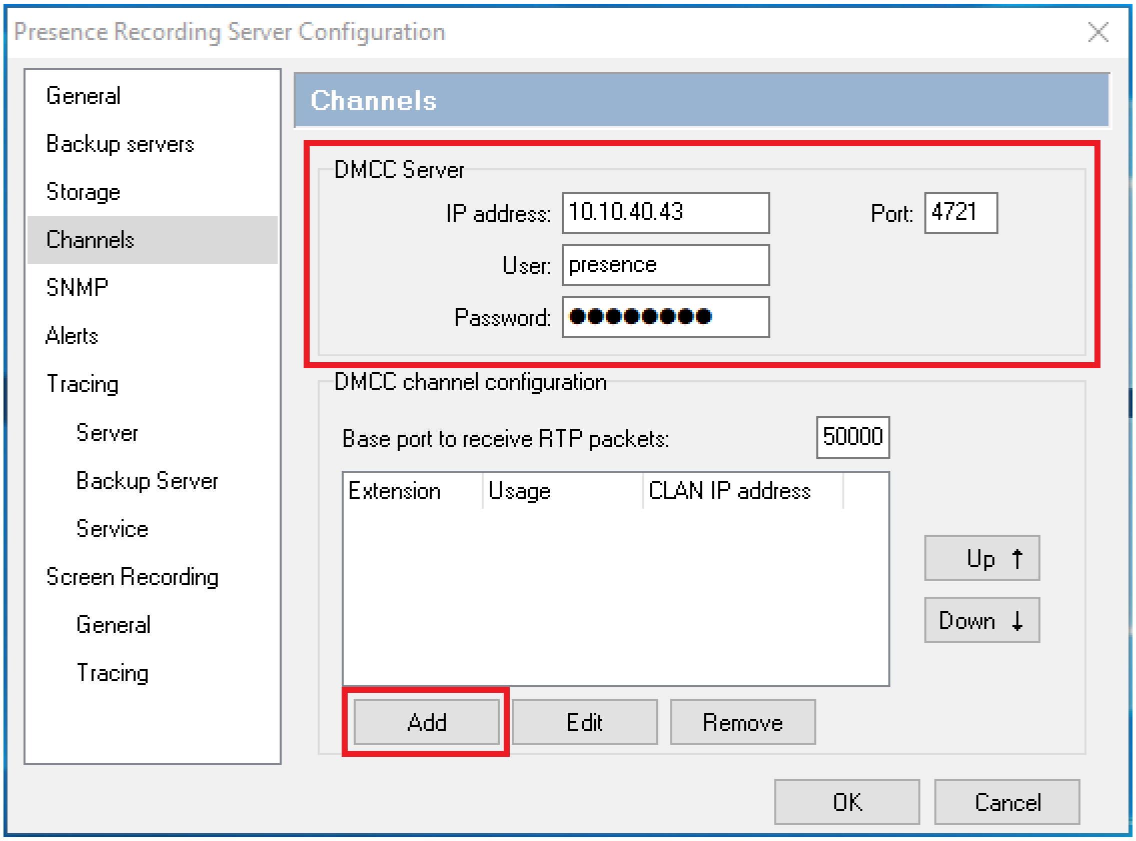
Space for recordings: 80 %

Space for retrieved recordings: 10 %

Minimum free space: 10 %

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**.



DMCC Server

IP address: 10.10.40.43

Port: 4721

User: presence

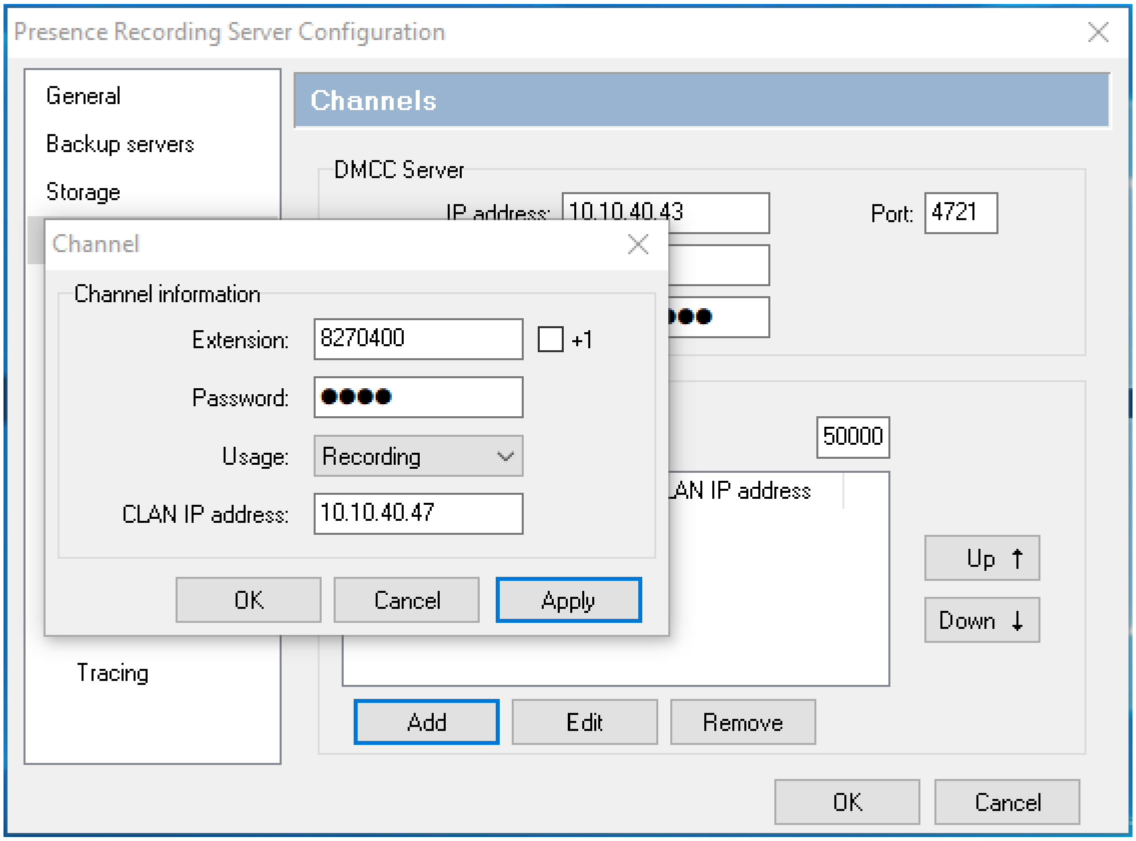
Password: ●●●●●●●●

DMCC channel configuration

Base port to receive RTP packets: 50000

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.



Channel information

Extension: 8270400 □ +1

Password: ●●●●

Usage: Recording

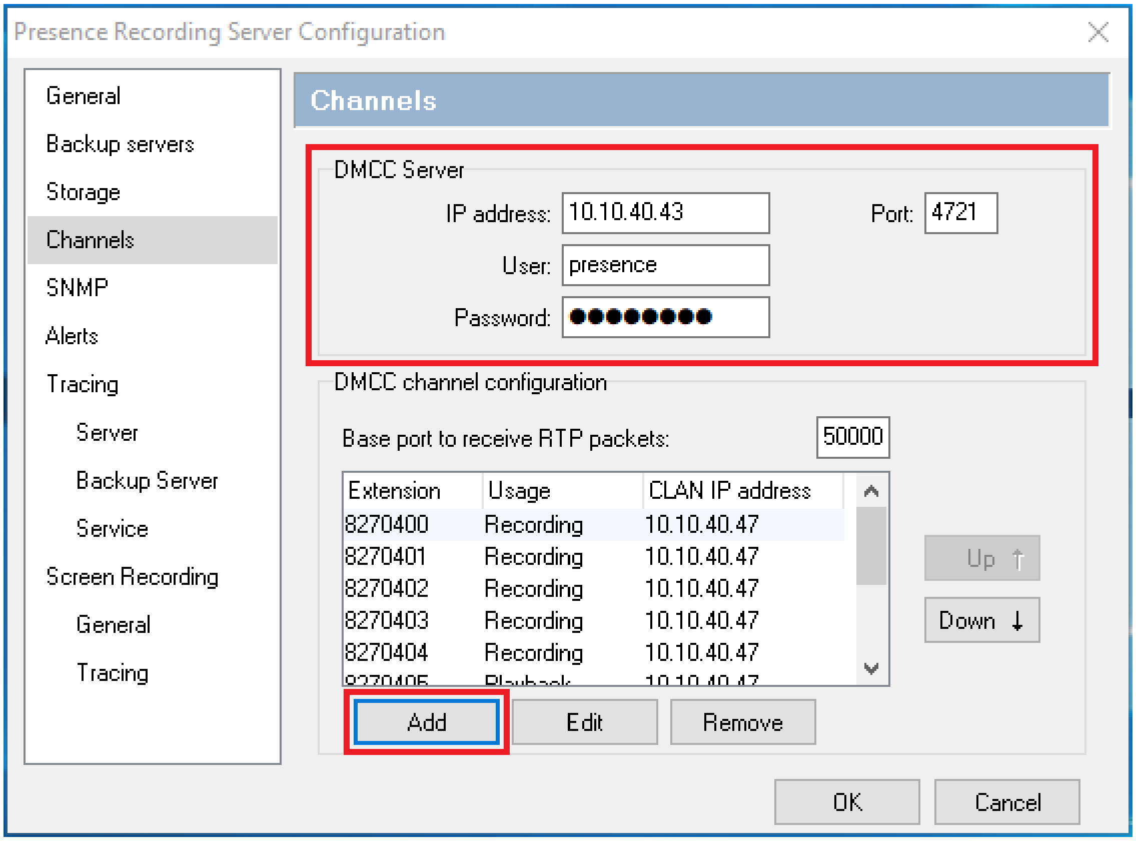
CLAN IP address: 10.10.40.47

DMCC Server

IP address: 10.10.40.43

Port: 4721

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



DMCC Server

IP address: 10.10.40.43 Port: 4721

User: presence

Password: ●●●●●●●●●

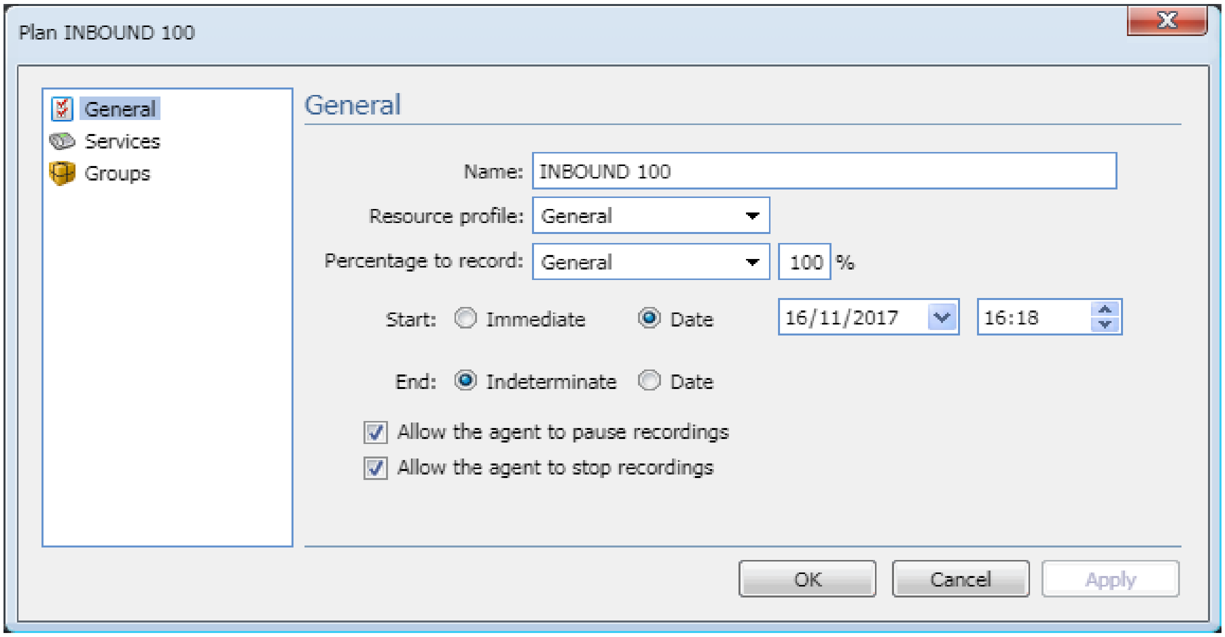
DMCC channel configuration

Base port to receive RTP packets: 50000

Extension	Usage	CLAN IP address
8270400	Recording	10.10.40.47
8270401	Recording	10.10.40.47
8270402	Recording	10.10.40.47
8270403	Recording	10.10.40.47
8270404	Recording	10.10.40.47
8270405	Playback	10.10.40.47

7.2. Configure Recording Plan

Recording plans must be configured according to the call recordings required. Using the Presence Web Supervisor, click on **Administration → Recording → Plans → New** (not shown). In the displayed 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.


Plan INBOUND 100

General

Name: INBOUND 100

Resource profile: General

Percentage to record: General 100 %

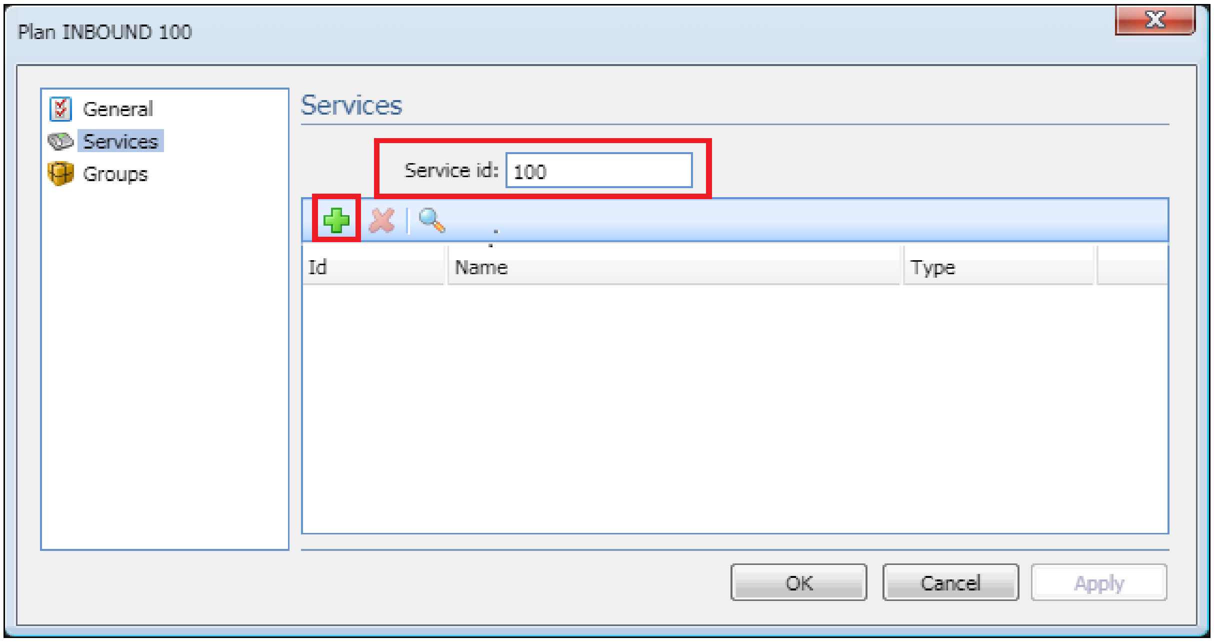
Start: ○ Immediate ● Date 16/11/2017 16:18

End: ● Indeterminate ○ Date

☑ Allow the agent to pause recordings

☑ Allow the agent to stop recordings

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

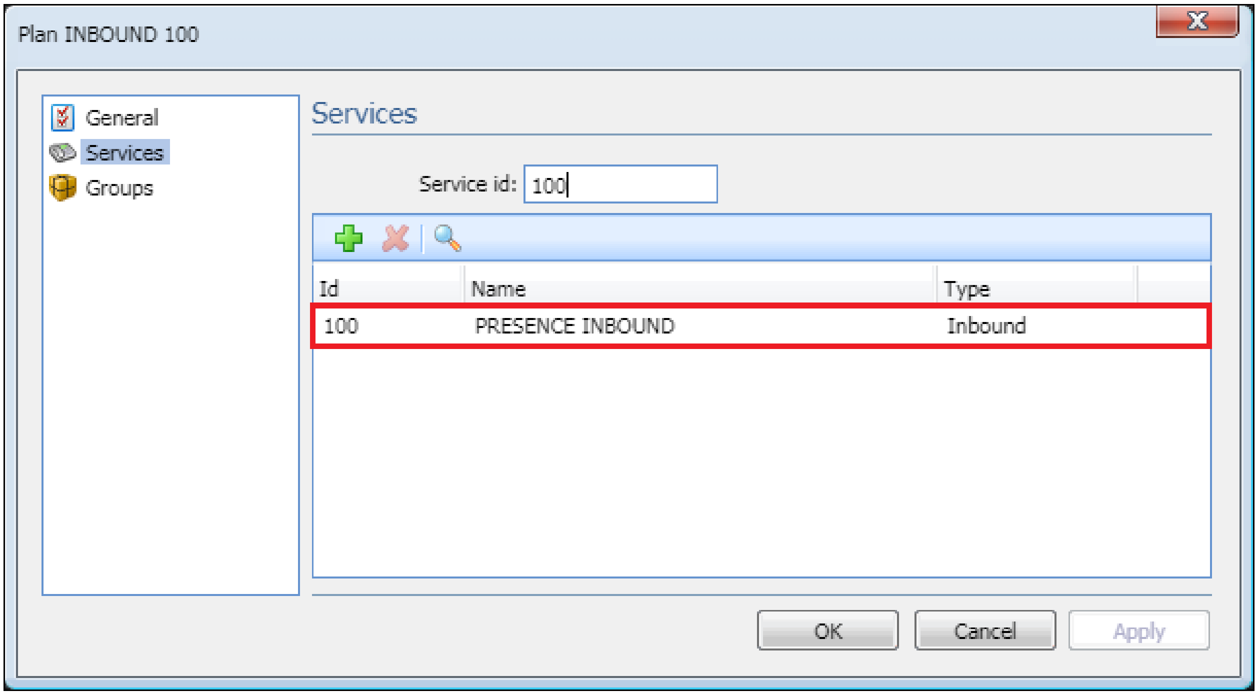

Plan INBOUND 100

Services

Service id: 100

Id	Name	Type

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



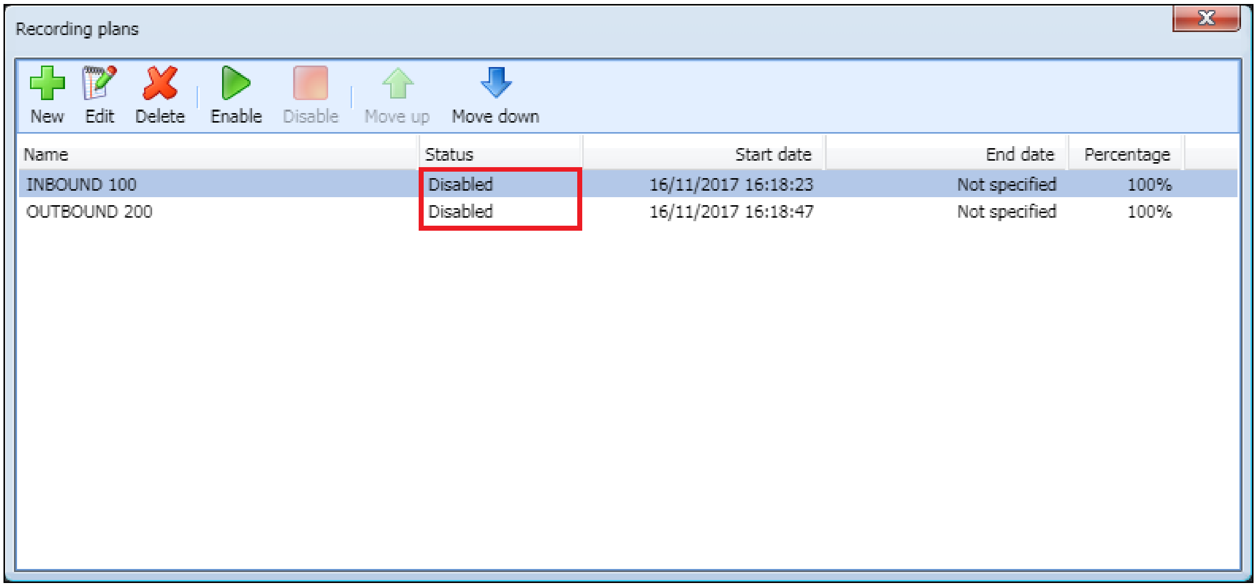
Plan INBOUND 100

Services

Service id: 100

Id	Name	Type
100	PRESENCE INBOUND	Inbound

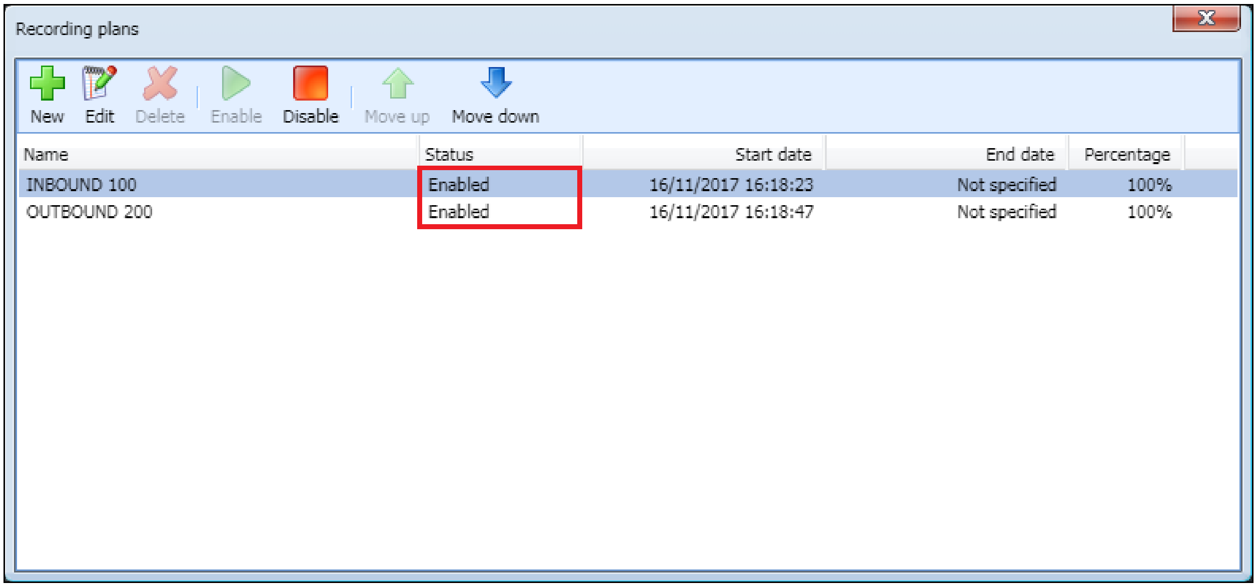
The screen below will be displayed, summarizing the added recording plans. Note that the status shows **Disabled**.



Recording plans

Name	Status	Start date	End date	Percentage
INBOUND 100	Disabled	16/11/2017 16:18:23	Not specified	100%
OUTBOUND 200	Disabled	16/11/2017 16:18:47	Not specified	100%

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



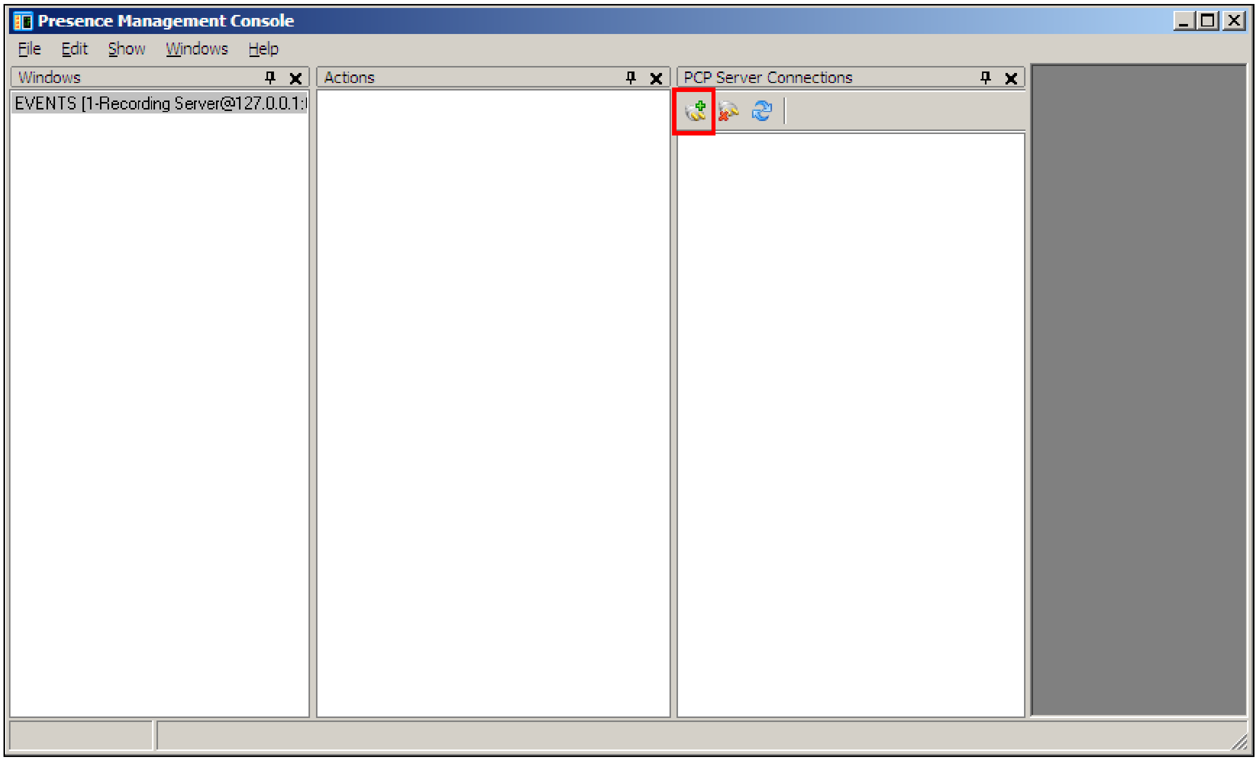
Name	Status	Start date	End date	Percentage
INBOUND 100	Enabled	16/11/2017 16:18:23	Not specified	100%
OUTBOUND 200	Enabled	16/11/2017 16:18:47	Not specified	100%

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

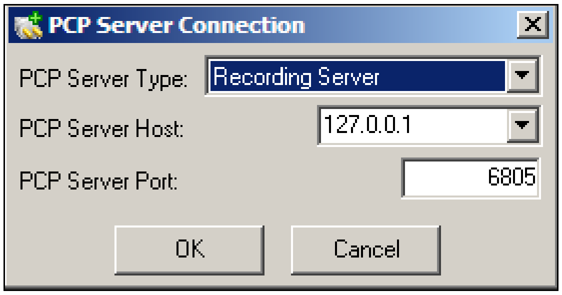
7.3. Add Avaya Aura® Communication Manager Stations to be Recorded

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.


Presence Management Console
File Edit Show Windows Help
Windows
EVENTS [1-Recording Server@127.0.0.1:
Actions
PCP Server Connections

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**.

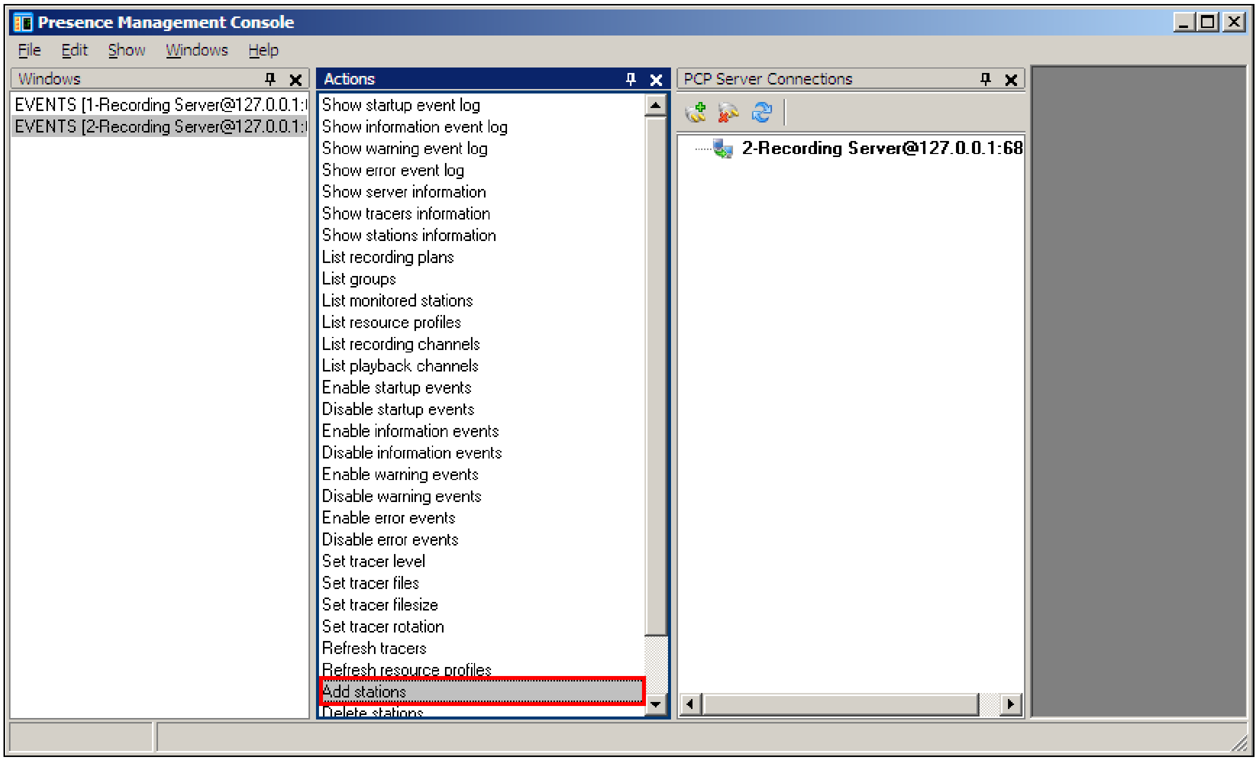


PCP Server Type: Recording Server

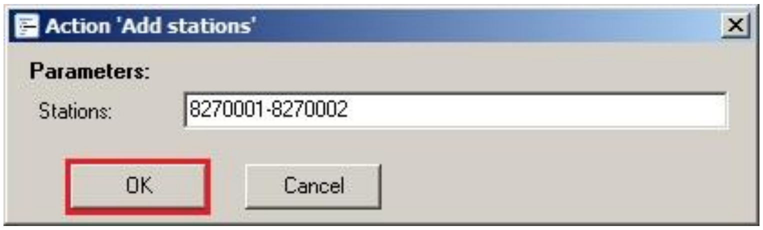
PCP Server Host: 127.0.0.1

PCP Server Port: 6805

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



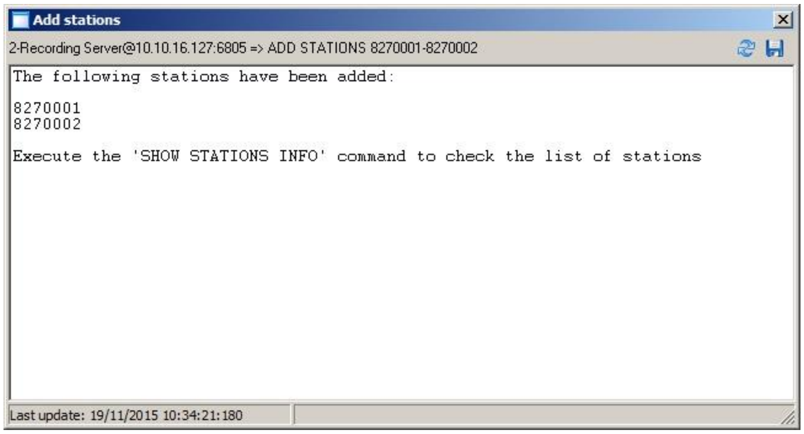
Enter the stations to be recorded and click **OK** when finished.



Parameters:

Stations: 8270001-8270002

The following screen appears showing the stations are added.

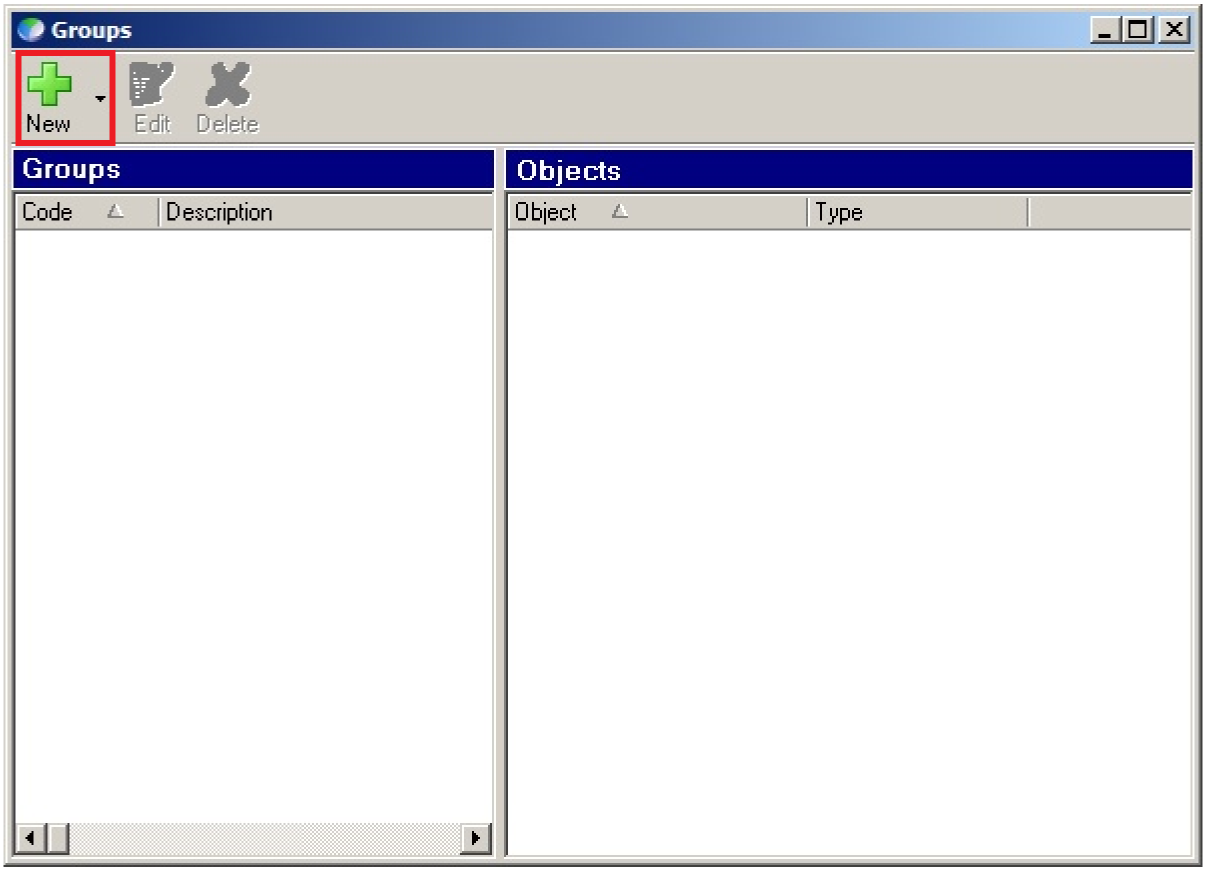


2-Recording Server@10.10.16.127:6805 => ADD STATIONS 8270001-8270002

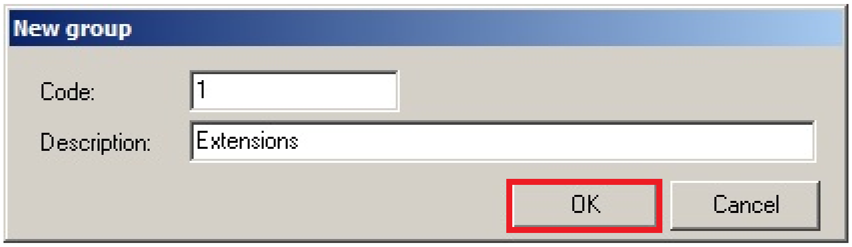
```
The following stations have been added:

8270001
8270002

Execute the 'SHOW STATIONS INFO' command to check the list of stations
```

Last update: 19/11/2015 10:34:21:180

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



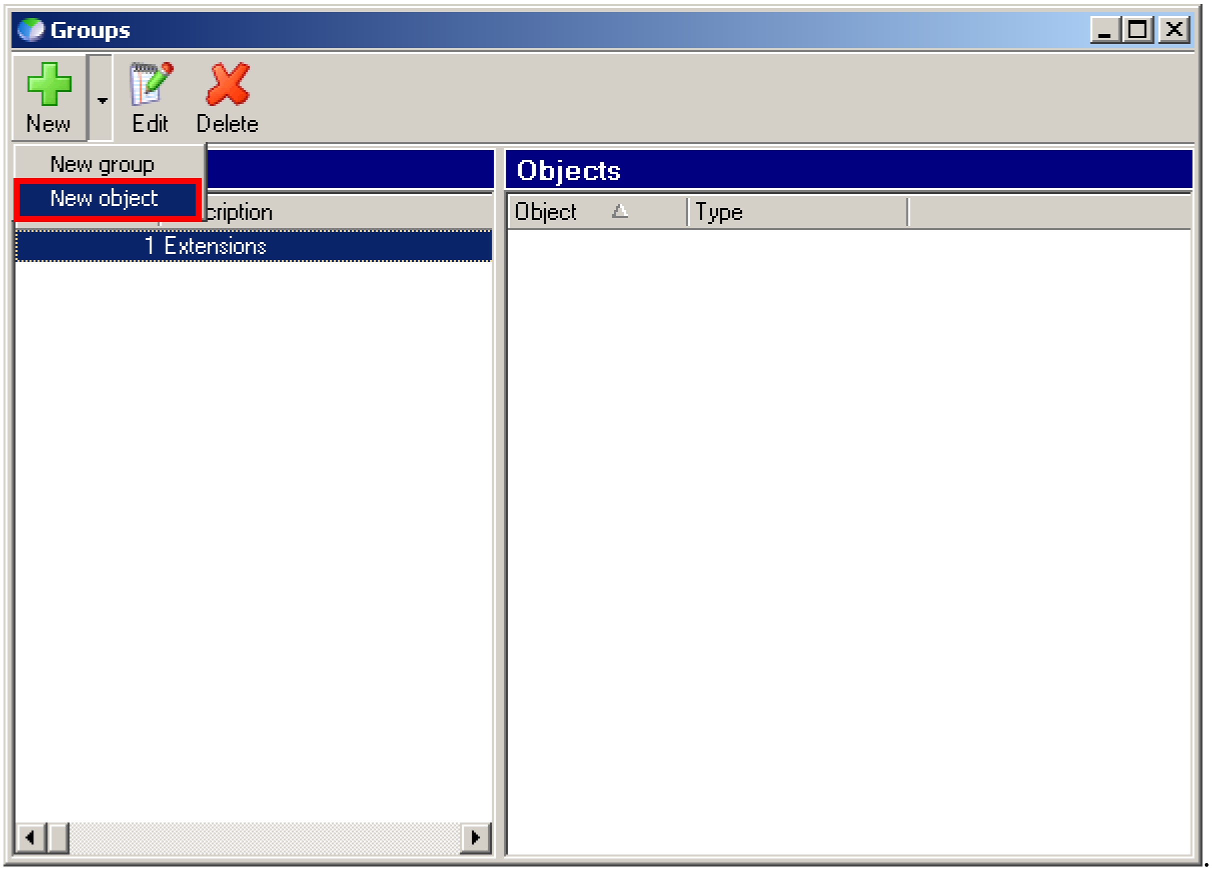
Enter the details for the new group. Note any number is used for code. Click on **OK** when finished.



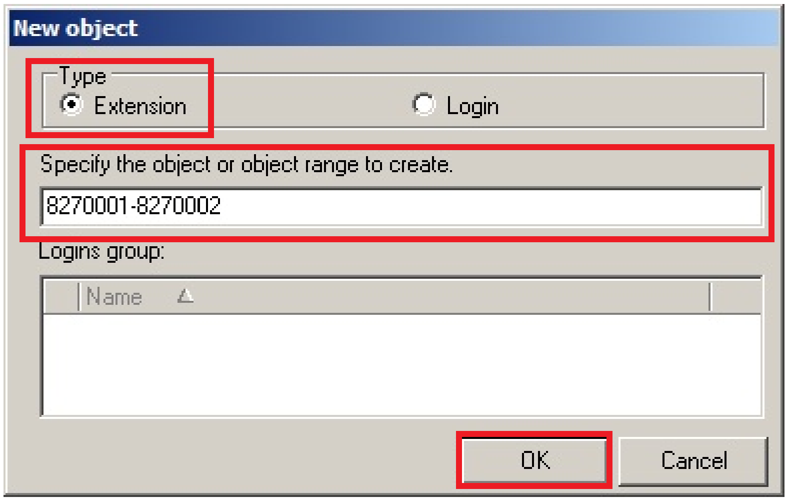
Code: 1

Description: Extensions

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.

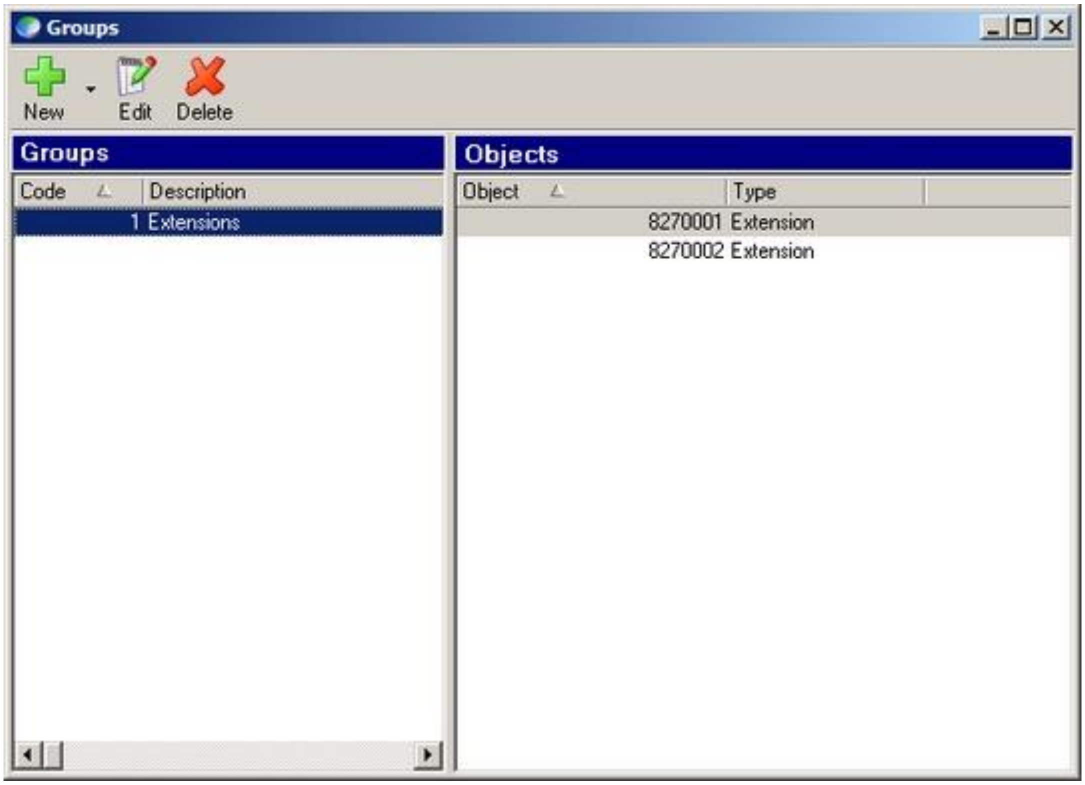


Type: ● Extension ○ Login

Specify the object or object range to create.

8270001-8270002

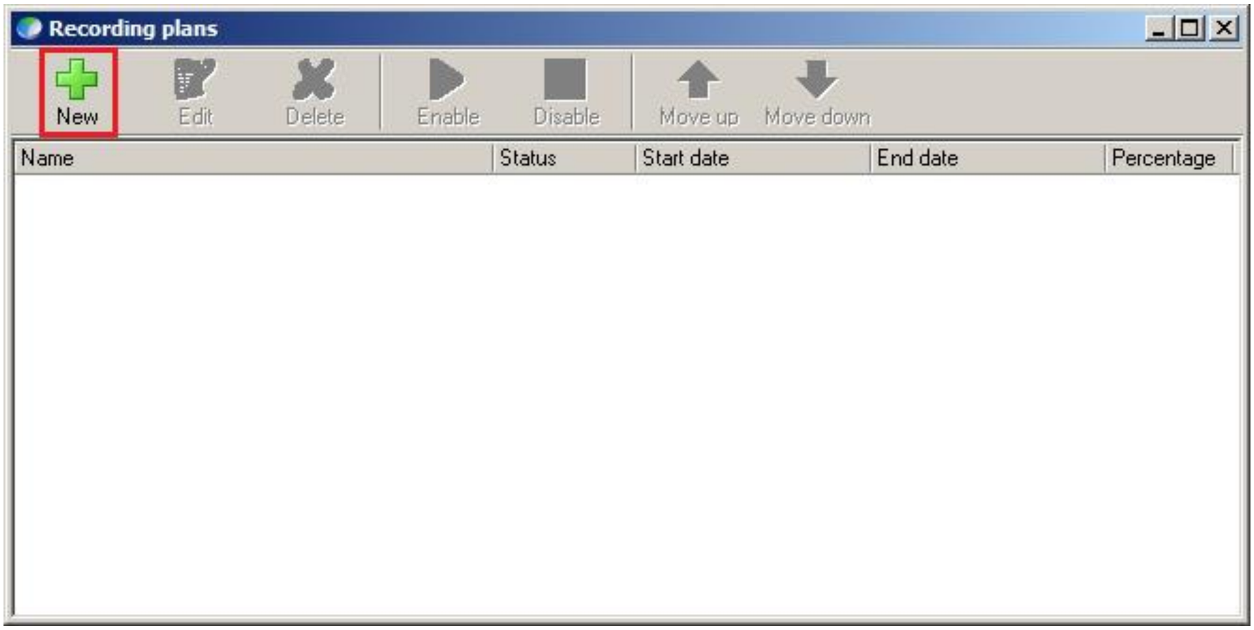
Once **OK** is clicked above, the following screen shows the added stations.



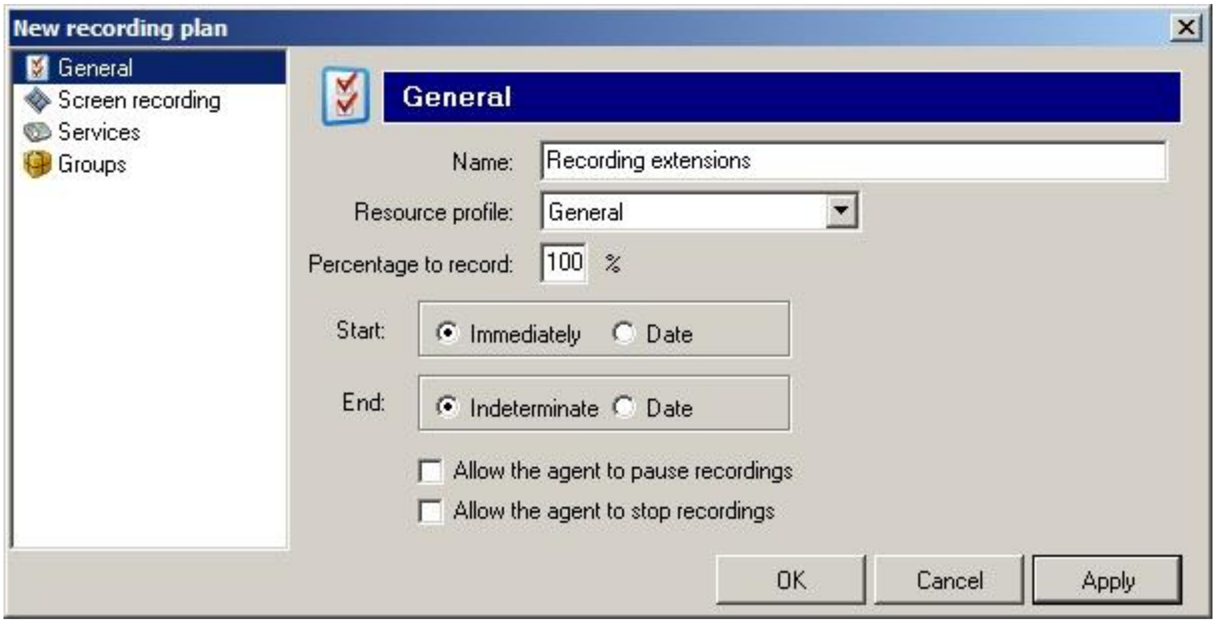
Code	Description
1	Extensions

Object	Type
8270001	Extension
8270002	Extension

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.



Name: Recording extensions

Resource profile: General

Percentage to record: 100 %

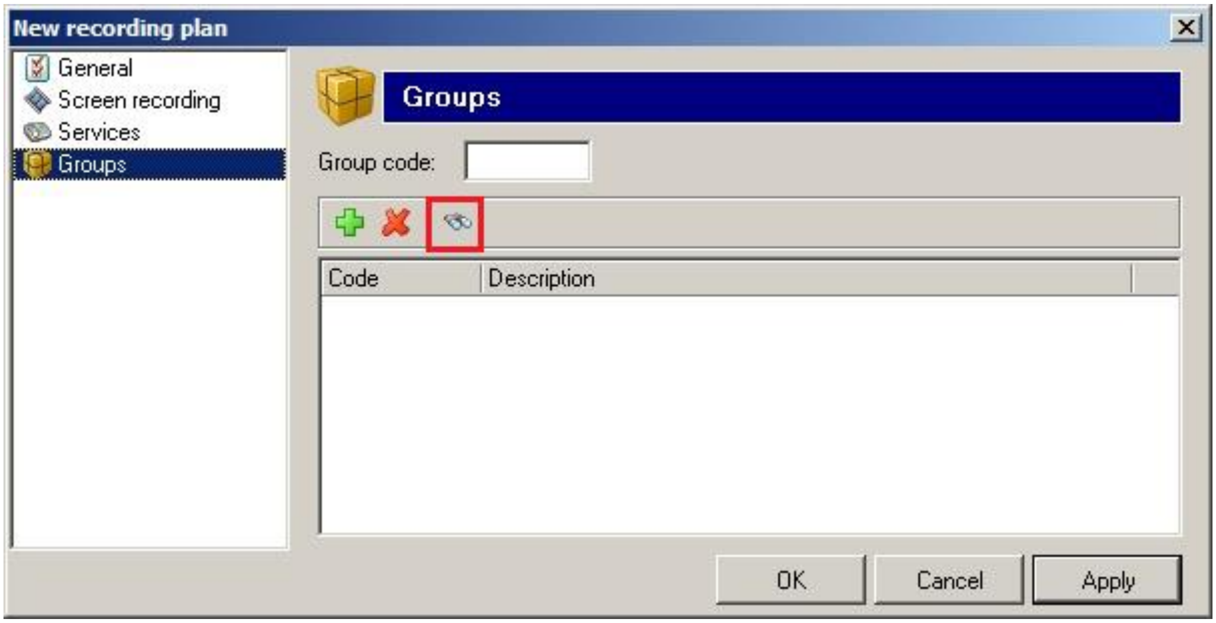
Start: ● Immediately ○ Date

End: ● Indeterminate ○ Date

□ Allow the agent to pause recordings

□ Allow the agent to stop recordings

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**.



Group code:

Code	Description

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

1          7        no      AES71vmpg        established    18        18
```

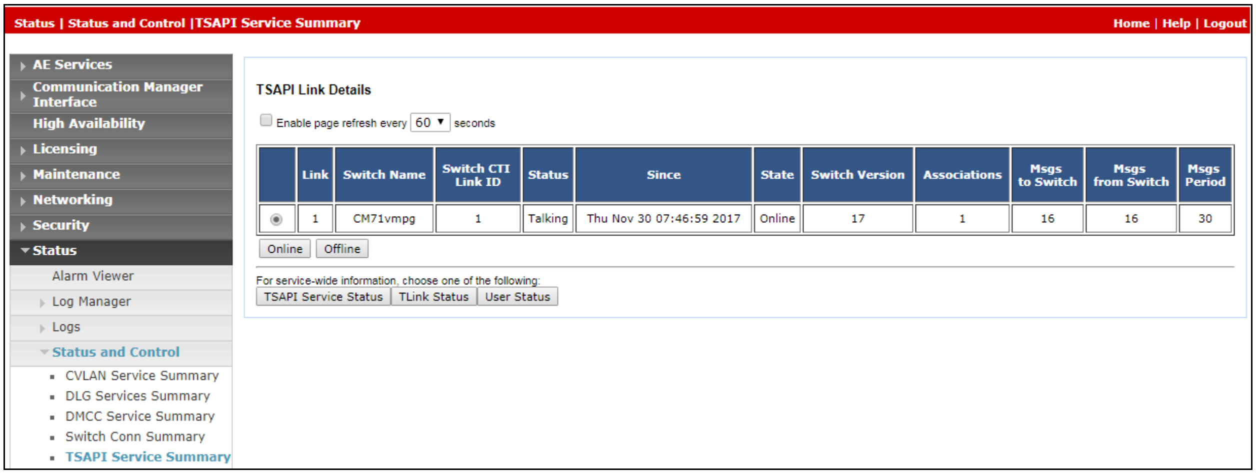
8.2. Verify TSAPI Link and DMCC

The following steps can be taken to ensure that the TSAPI and DMCC links are up and working properly with Presence Recording.

Note: The following screens serve as an example of what the connection should show. The IP addresses may be different depending on the site.

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**.



TSAPI Link Details

□ Enable page refresh every 60 ▼ seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	CM71vmpg	1	Talking	Thu Nov 30 07:46:59 2017	Online	17	1	16	16	30

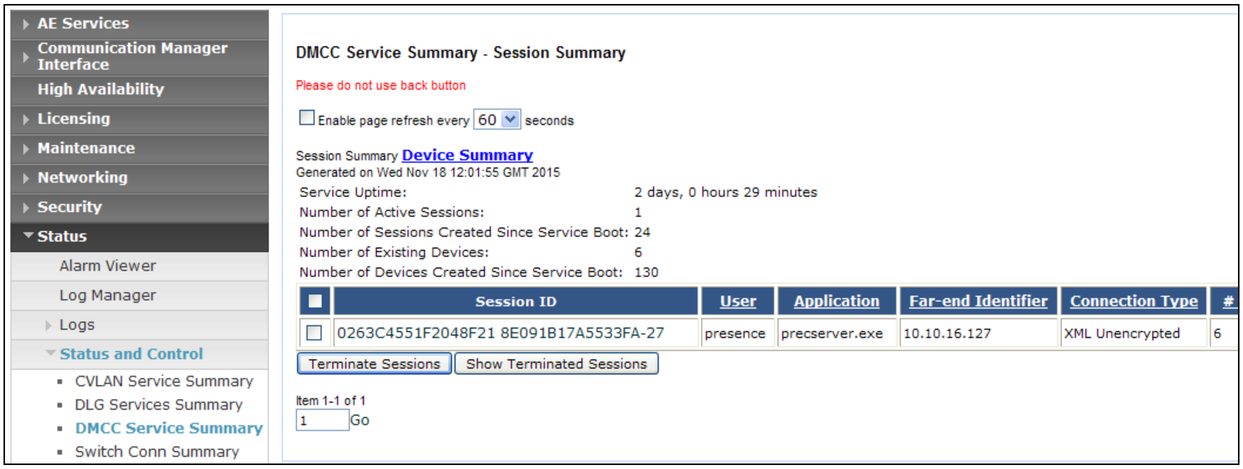
Online | Offline

For service-wide information, choose one of the following:

TSAPI Service Status | TLink Status | 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**.



DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Wed Nov 18 12:01:55 GMT 2015

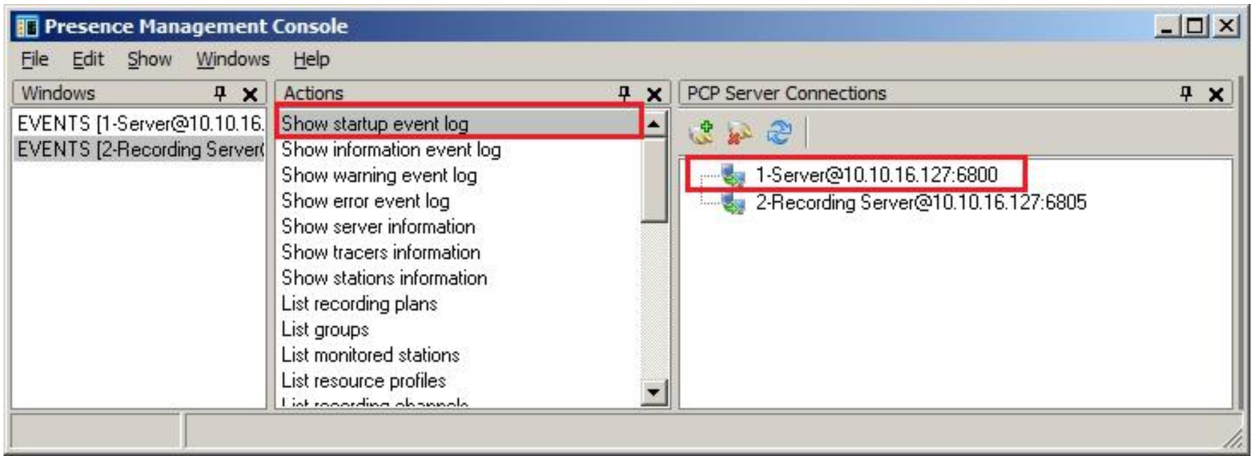
```
Service Uptime:                              2 days, 0 hours 29 minutes
Number of Active Sessions:                   1
Number of Sessions Created Since Service Boot: 24
Number of Existing Devices:                  6
Number of Devices Created Since Service Boot: 130
```

■	Session ID	User	Application	Far-end Identifier	Connection Type	#
□	0263C4551F2048F21 8E091B17A5533FA-27	presence	precserver.exe	10.10.16.127	XML Unencrypted	6

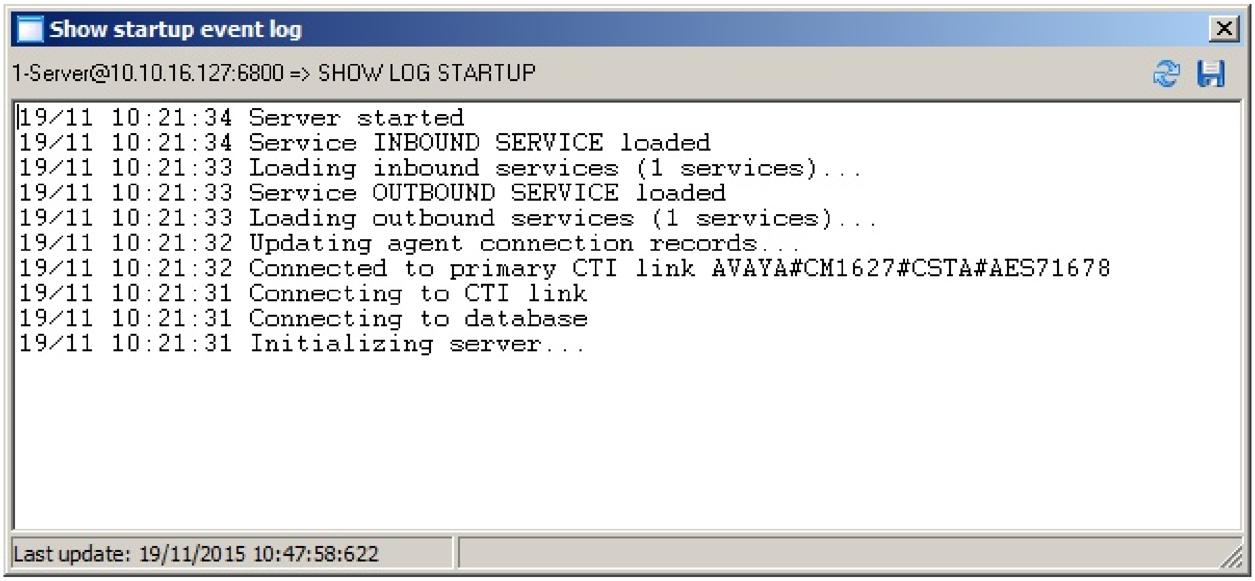
Item 1-1 of 1
1 Go

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.

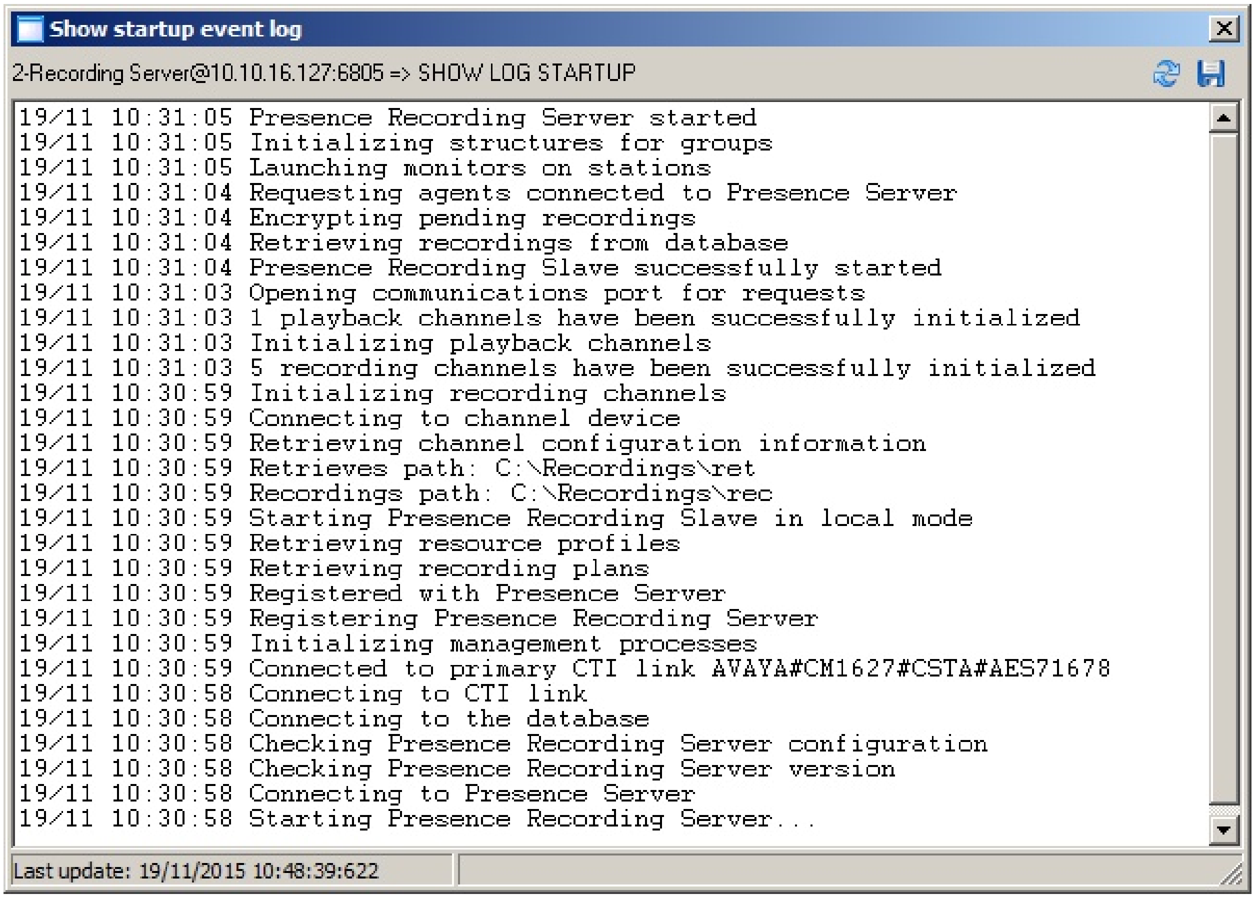


1-Server@10.10.16.127:6800 => SHOW LOG STARTUP

```
19/11 10:21:34 Server started
19/11 10:21:34 Service INBOUND SERVICE loaded
19/11 10:21:33 Loading inbound services (1 services)...
19/11 10:21:33 Service OUTBOUND SERVICE loaded
19/11 10:21:33 Loading outbound services (1 services)...
19/11 10:21:32 Updating agent connection records...
19/11 10:21:32 Connected to primary CTI link AVAYA#CM1627#CSTA#AES71678
19/11 10:21:31 Connecting to CTI link
19/11 10:21:31 Connecting to database
19/11 10:21:31 Initializing server...
```

Last update: 19/11/2015 10:47:58:622

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



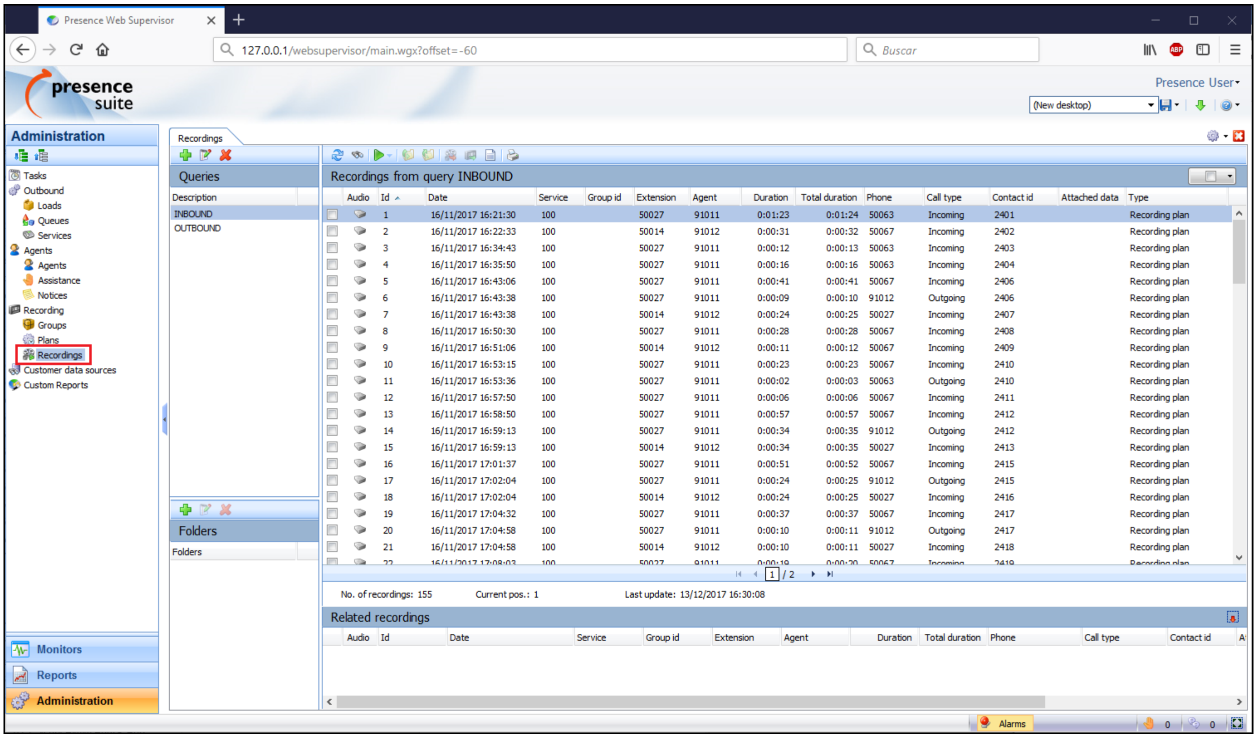
2-Recording Server@10.10.16.127:6805 => SHOW LOG STARTUP

```
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 Web Supervisor, click **Administration → Recording → Recordings**, visually verify correct recording detail as shown below.



Recordings from query INBOUND

	Audio	Id	Date	Service	Group id	Extension	Agent	Duration	Total duration	Phone	Call type	Contact id	Attached data	Type
□		1	16/11/2017 16:21:30	100		50027	91011	0:01:23	0:01:24	50063	Incoming	2401		Recording plan
□		2	16/11/2017 16:22:33	100		50014	91012	0:00:31	0:00:32	50067	Incoming	2402		Recording plan
□		3	16/11/2017 16:34:43	100		50027	91011	0:00:12	0:00:13	50063	Incoming	2403		Recording plan
□		4	16/11/2017 16:35:50	100		50027	91011	0:00:16	0:00:16	50063	Incoming	2404		Recording plan
□		5	16/11/2017 16:43:06	100		50027	91011	0:00:41	0:00:41	50067	Incoming	2406		Recording plan
□		6	16/11/2017 16:43:38	100		50027	91011	0:00:09	0:00:10	91012	Outgoing	2406		Recording plan
□		7	16/11/2017 16:43:38	100		50014	91012	0:00:24	0:00:25	50027	Incoming	2407		Recording plan
□		8	16/11/2017 16:50:30	100		50027	91011	0:00:28	0:00:28	50067	Incoming	2408		Recording plan
□		9	16/11/2017 16:51:06	100		50014	91012	0:00:11	0:00:12	50067	Incoming	2409		Recording plan
□		10	16/11/2017 16:53:15	100		50027	91011	0:00:23	0:00:23	50067	Incoming	2410		Recording plan
□		11	16/11/2017 16:53:36	100		50027	91011	0:00:02	0:00:03	50063	Outgoing	2410		Recording plan
□		12	16/11/2017 16:57:50	100		50027	91011	0:00:06	0:00:06	50067	Incoming	2411		Recording plan
□		13	16/11/2017 16:58:50	100		50027	91011	0:00:57	0:00:57	50067	Incoming	2412		Recording plan
□		14	16/11/2017 16:59:13	100		50027	91011	0:00:34	0:00:35	91012	Outgoing	2412		Recording plan
□		15	16/11/2017 16:59:13	100		50014	91012	0:00:34	0:00:35	50027	Incoming	2413		Recording plan
□		16	16/11/2017 17:01:37	100		50027	91011	0:00:51	0:00:52	50067	Incoming	2415		Recording plan
□		17	16/11/2017 17:02:04	100		50027	91011	0:00:24	0:00:25	91012	Outgoing	2415		Recording plan
□		18	16/11/2017 17:02:04	100		50014	91012	0:00:24	0:00:25	50027	Incoming	2416		Recording plan
□		19	16/11/2017 17:04:32	100		50027	91011	0:00:37	0:00:37	50067	Incoming	2417		Recording plan
□		20	16/11/2017 17:04:58	100		50027	91011	0:00:10	0:00:11	91012	Outgoing	2417		Recording plan
□		21	16/11/2017 17:04:58	100		50014	91012	0:00:10	0:00:11	50027	Incoming	2418		Recording plan
□		22	16/11/2017 17:08:03	100		50027	91011	0:00:19	0:00:20	50067	Incoming	2419		Recording plan

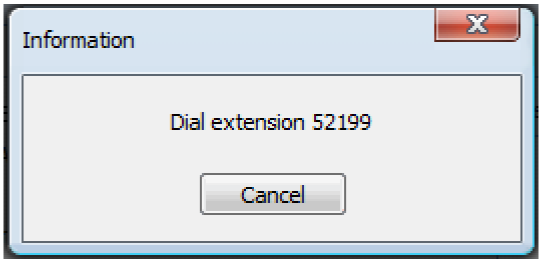
1 / 2

No. of recordings: 155　Current pos.: 1　Last update: 13/12/2017 16:30:08

Related recordings

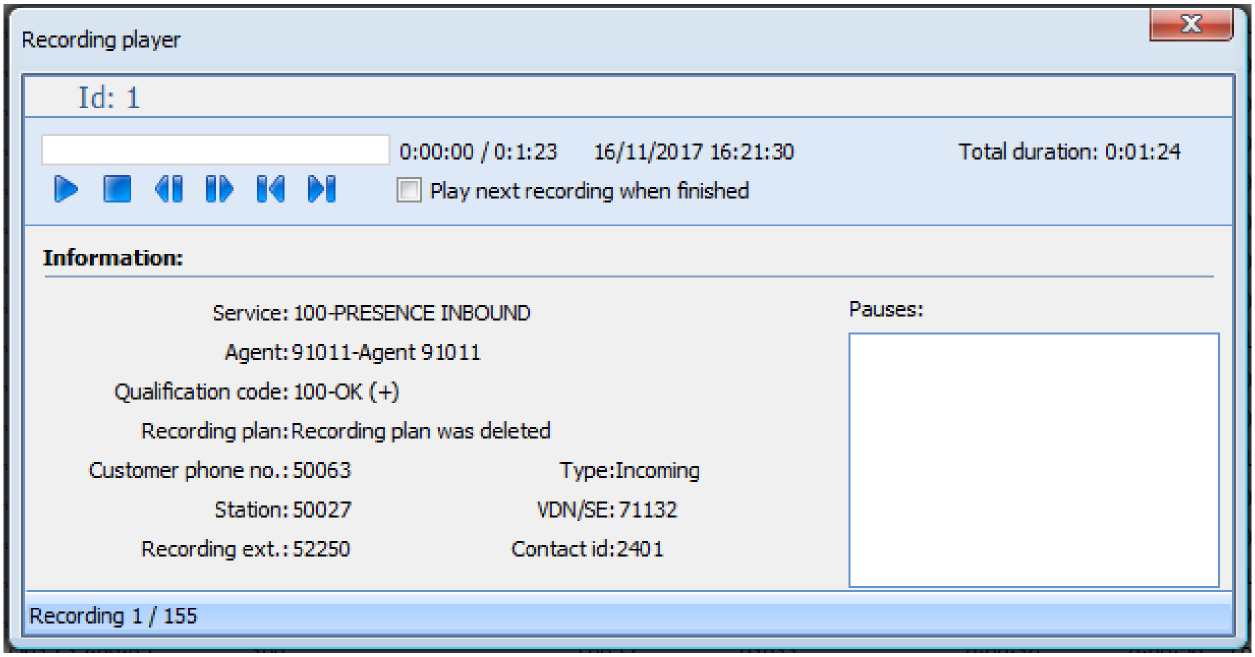
	Audio	Id	Date	Service	Group id	Extension	Agent	Duration	Total duration	Phone	Call type	Contact id	A

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


Information

Dial extension 52199

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



0:00:00 / 0:1:23 16/11/2017 16:21:30 Total duration: 0:01:24

□ Play next recording when finished

Information:

Service: 100-PRESENCE INBOUND

Agent: 91011-Agent 91011

Qualification code: 100-OK (+)

Recording plan: Recording plan was deleted

Customer phone no.: 50063 Type: Incoming

Station: 50027 VDN/SE: 71132

Recording ext.: 52250 Contact id: 2401

Pauses:

Recording 1 / 155

9. Conclusion

These Application Notes describe the configuration steps required for Presence Technology Presence Recording R11.0 to successfully interoperate with Avaya Aura® Communication Manager R7.1 using Avaya Aura® Application Enablement Services R7.1. 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 7.1*

The following documentation is available on request from Presence: www.presenceco.com

[4] *ACD Sys Presence Administrator Manual Presence Suite*, V11.0

[5] *Presence Installation Guides Presence Software*, V11.0

[6] *PBX/ACD Requirements Presence Software*, V11.0

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.