



Avaya Solution & Interoperability Test Lab

Application Notes for Envision Click2Coach with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services for Full Time Recording with Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Envision Click2Coach to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services for Full Time Recording with Service Observing. Envision Click2Coach is a call recording solution.

In the compliance testing, Envision Click2Coach used the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to monitor contact center agents on Avaya Aura® Communication Manager, and obtain call information and media associated with the monitored agents for call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 configuration steps required for Envision Click2Coach to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES) for Full Time Recording with Service Observing. Envision Click2Coach is a call recording solution.

In the compliance testing, Envision Click2Coach used the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to monitor contact center agents on Avaya Aura® Communication Manager, and obtain call information and media associated with the monitored agents for call recording.

In a Full Time Recording environment, all calls at the monitored agents are recorded. Envision Click2Coach uses the DMCC interface to monitor calls at the agents, and to obtain the media associated with the calls for recording. The media is obtained by using the Service Observing feature to enable a virtual IP softphone to observe and join active calls at the agent.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Envision Click2Coach application, the application uses Avaya Aura® Application Enablement Services DMCC to automatically register the virtual IP softphones to Avaya Aura® Communication Manager, request monitoring on the stations to be recorded, and initiate Service Observing from the virtual IP softphones.

For the manual part of the testing, each call was handled manually on the station user with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the user telephones to test the different call scenarios for softphone and hard phone. It also includes feature calls such as transfer, conference and bridging.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to Envision Click2Coach, restarting DMCC service on the AES, busying and releasing CTI link on the Communication Manager, restarting Communication Manager and finally restarting the AES server.

The verification of tests included using the Envision Click2Coach logs for proper message exchanges, using the Envision thin client web interface to verify proper logging and playing back of the calls.

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 feature and serviceability testing.

Feature testing focused on verifying the following on Envision Click2Coach proper recordings, loggings and playback of calls:

- Inbound calls, external and internal calls
- Outbound calls, external and internal calls
- Bridge calls
- Transfer calls
- Conference calls
- ACD and non-ACD calls
- Call Hold and Resume
- Hard phone and Softphone with one-X Agent

Serviceability testing focused on verifying the ability of Envision Click2Coach to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to Envision Click2Coach server, DMCC service and restarting the CTI link as well as AES and Communication Manager server.

2.2. Test Results

All feature test cases were successfully completed with the following observations:

- Voice recordings not functioning after reconnecting server LAN network for disconnect time of 90 secs in the serviceability test. Voice recordings do function well for disconnect time of 30 and 130 secs.
- KeepAlive missed messages appear in the Envision server logs repeatedly after DMCC service restarts. The Envision Channel Manager service needs to be restarted to clear this error.
- Multiple calls at the same agent are lumped into one call recording by design.
- In a failed Service Observing scenario, the recording contains the denial tone followed by silence.

2.3. Support

Technical support on Envision Click2Coach can be obtained through the following:

- **Phone:** 1-800-975-9384
- **Email:** support@envisioninc.com
- **Web:** <http://www.envisioninc.com/>

3. Reference Configuration

Envision Click2Coach has a thin client web interface that can be used to review and playback the call recordings.

In the compliance testing, Envision Click2Coach monitored the agent station extensions shown in the contact center device table below.

Device Type	Extension
VDN	14001
Skill Group	13001
Supervisor Station	10001
Agent Station	10001 → 10005
Agent ID	11001 → 11005
Virtual Station DMCC	19901 → 19905

Figure 1 on the next page illustrates the test configuration consisting of a duplex pair of Avaya Aura® Communication Manager servers, Avaya G430 Media Gateway, Avaya Aura® AES Server and Avaya Aura® Media Server. Avaya 96x1, 96x0 and 1600 Series H.323 IP Deskphones including 9400 Series Digital Deskphone are used as agent stations. Avaya 1400 Series Digital Deskphone serves as a non-recorded station. Envision server is installed on Microsoft Windows 2012 R2 which communicates with the TSAPI Service on the Avaya Aura® AES Server. The Avaya 4548GT-PWR Converged Stackable Switch provides ethernet connectivity to the servers and IP telephones. A simulated public PSTN trunk connects to the system. The telephones will be used to generate intraswitch calls (calls between telephones on the same system) and outbound/inbound calls to/from the PSTN.

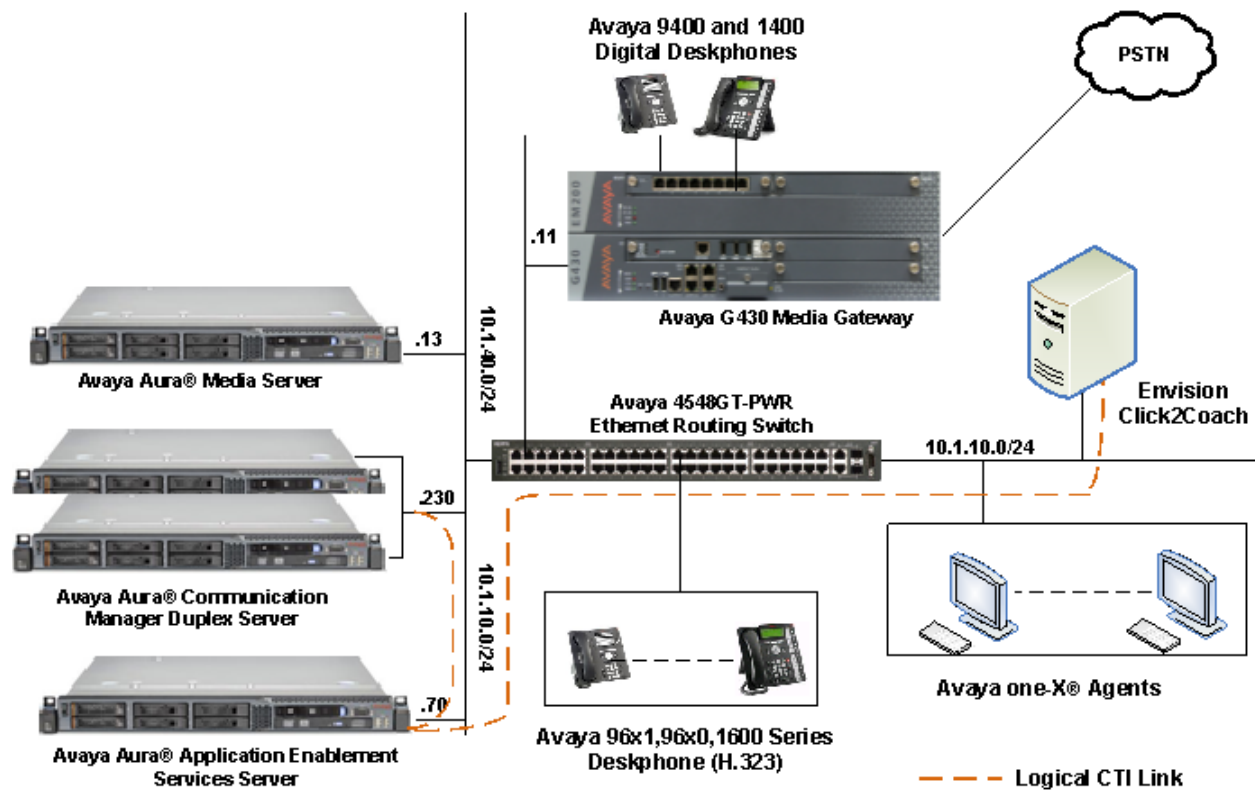


Figure 1: Test Configuration

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 (Duplex)	7.0.1.1.1 (Service Pack 1.1) (R017x.00.0.441.0-23384)
Avaya S8300D Server (w/ G430) running Avaya Aura® Communication Manager	7.0.1.1.1 (Service Pack 1.1) (R017x.00.0.441.0-23384)
Avaya G430 Media Gateway: MM712AP (DCP)	HW04 FW015
Avaya Aura® Application Enablement Services (AES) Server	7.0 (7.0.1.0.3.15-0)
Avaya Aura® Media Server	7.7.0.19
Avaya 4548GT-PWR Converged Stackable Switch	5.3.0.3
Avaya 1600 Series IP Phones : 1608 (H.323)	1.380A
Avaya 96x0 Series IP Phones: 9630 (H.323)	3.250A
Avaya 96x1 Series IP Phones: 9611 (H.323) 9641 (H.323)	6.6029 6.6029
Avaya 9400 Series Digital Phones	2.0.SP4
Avaya 1400 Series Digital Phones	Rel 4 SP7
Avaya one-X® Agent running on Windows 10 Professional	2.5.58020.604
Envision Click2Coach on Windows 2012 R2 Server <ul style="list-style-type: none">Envision Click2CoachEnvision ServerEnvision CTC Loader	11.5.1.159 10.2.35.3 1.3.3

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager License
- Administer System Parameters Features
- Administer AES and CTI link
- Administer Class of Restriction
- Administer Agent Stations
- Administer Virtual IP softphones

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** customer option is set to **y** on **Page 4**. If this option is not set to **y**, then contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                               Page 4 of 12
                                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? n      DCS (Basic)? y
ASAI Link Core Capabilities? y      DCS Call Coverage? y
ASAI Link Plus Capabilities? y      DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n      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

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

5.2. Administer System Parameters Features

Use the **change system-parameters features** command to enable **Allow Two Observers in Same Call**, which is located on **Page 11**.

change system-parameters features		Page 11 of 19
FEATURE-RELATED SYSTEM PARAMETERS		
CALL CENTER SYSTEM PARAMETERS		
EAS		
Expert Agent Selection (EAS) Enabled? y		
Minimum Agent-LoginID Password Length:		
Direct Agent Announcement Extension:		Delay:
Message Waiting Lamp Indicates Status For: station		
VECTORIZING		
Converse First Data Delay: 0		Second Data Delay: 2
Converse Signaling Tone (msec): 100		Pause (msec): 70
Prompting Timeout (secs): 10		
Interflow-qpos EWT Threshold: 2		
Reverse Star/Pound Digit For Collect Step? y		
Available Agent Adjustments for BSR? n		
BSR Tie Strategy: 1st-found		
Store VDN Name in Station's Local Call Log? n		
SERVICE OBSERVING		
Service Observing: Warning Tone? y		or Conference Tone? n
Allowed with Exclusion: Service Observing? n		SSC? n
Allow Two Observers in Same Call? y		

5.3. Administer AES and CTI Link

Enter the **change node-names ip procr** command. In the compliance-tested configuration, note the ip address of the Communication Manager with the node-name **procr** was utilized for connectivity to Avaya AES server.

change node-names ip procr		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
procr	10.1.10.230	
procr6	::	

Enter the **change ip-services** command. On **Page 1**, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. The **Local Node** field should be set to the **procr**. During the compliance test, the default port was utilized for the **Local Port** field.

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

On **Page 4**, enter the hostname of the Avaya AES server for the **AE Services Server** field. The server name may be obtained by logging in to the Avaya AES server using Secure Shell (SSH) and running the **uname -a** command. Enter an alphanumeric password for the **Password** field and set the **Enabled** field to **y**. The same password will be configured on Avaya AES server in **Section 6.3**.

change ip-services				Page	4 of	4
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:						
2:	aes7x	xxxxxxxxxxxxxxxxxx	y			

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

add cti-link 3			Page	1 of	3
CTI LINK					
CTI Link: 3					
Extension: 10093					
Type: ADJ-IP					
Name: TSAPI Service - AES7x			COR: 1		

5.4. Administer Class of Restriction

Enter the **change cor n** command, where **n** is the class of restriction (COR) number used for integration with Envision. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to **y**, as shown below. For the compliance testing, this COR was assigned to the physical stations used by the agents and to the virtual IP softphones used by Envision.

change cor 1		Page 1 of 23	
CLASS OF RESTRICTION			
COR Number: 1			
COR Description: All Users			
FRL: 0		APLT? y	
Can Be Service Observed? y		Calling Party Restriction: none	
Can Be A Service Observer? y		Called Party Restriction: none	
Time of Day Chart: 1		Forced Entry of Account Codes? n	
Priority Queuing? n		Direct Agent Calling? y	
Restriction Override: none		Facility Access Trunk Test? n	
Restricted Call List? n		Can Change Coverage? n	
Access to MCT? y		Fully Restricted Service? n	
Group II Category For MFC: 7		Hear VDN of Origin Annc.? y	
Send ANI for MFE? n		Add/Remove Agent Skills? n	
MF ANI Prefix:		Automatic Charge Display? n	
Hear System Music on Hold? y		PASTE (Display PBX Data on Phone)? n	
Can Be Picked Up By Directed Call Pickup? n		Can Use Directed Call Pickup? n	
Group Controlled Restriction: inactive			

5.5. Administer Agent Stations

Modify each physical station used by the agents to allow the station to be service observed. Change the agent station using the **change station n** command, where **n** is the station extension number. For the COR field, enter the COR from **Section 5.4**, which allows the station to be service observed.

Repeat this section for all agent stations in **Section 2**.

change station 10001		Page 1 of 5
STATION		
Extension: 10001	Lock Messages? n	BCC: 0
Type: 9611G	Security Code: 111222	TN: 1
Port: S00002	Coverage Path 1:	COR: 1
Name: IP Station 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 10001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

5.6. Administer Virtual IP Softphones

Add a virtual softphone using the **add station n** command, where **n** is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** Any IP telephone type allowing multiple buttons, such as **4624**.
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **COR:** The class of restriction number from **Section 5.4**.
- **IP SoftPhone:** Set to **y**.

add station 19901		Page 1 of 6
STATION		
Extension: 19901	Lock Messages? n	BCC: 0
Type: 4624	Security Code: 19901	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: DMCC #1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 19901	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

Navigate to **Page 4**, and assign a **serv-obsrv** button for activation of the Service Observing feature. Make a note of the button number, in this case **4**, as this will be used later to configure Envision. Also note that the same button number should be used for all virtual softphones.

```
change station 19901
```

Page 4 of 6

STATION

SITE DATA

Room:	Headset? n
Jack:	Speaker? n
Cable:	Mounting: d
Floor:	Cord Length: 0
Building:	Set Color:

ABBREVIATED DIALING

List1:	List2:	List3:
--------	--------	--------

BUTTON ASSIGNMENTS

1: call-appr	7:
2: call-appr	8:
3: call-appr	9:
4: serv-obsrv	10:
5:	11:
6:	12:

Repeat this section to administer the desired number of virtual IP softphones. In the compliance testing, 5 virtual IP softphones were administered as shown below for monitoring of administered agent stations in **Section 2**.

```
list station 19901 count 5
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack		
19901	S00395 4624	DMCC #1	no			1			
19902	S00006 4624	DMCC #2	no			1	1		
19903	S00007 4624	DMCC #3	no			1	1		
19904	S00008 4624	DMCC #4	no			1	1		
19905	S00011 4624	DMCC #5	no			1	1		

6. Configure Avaya Aura® Application Enablement Services

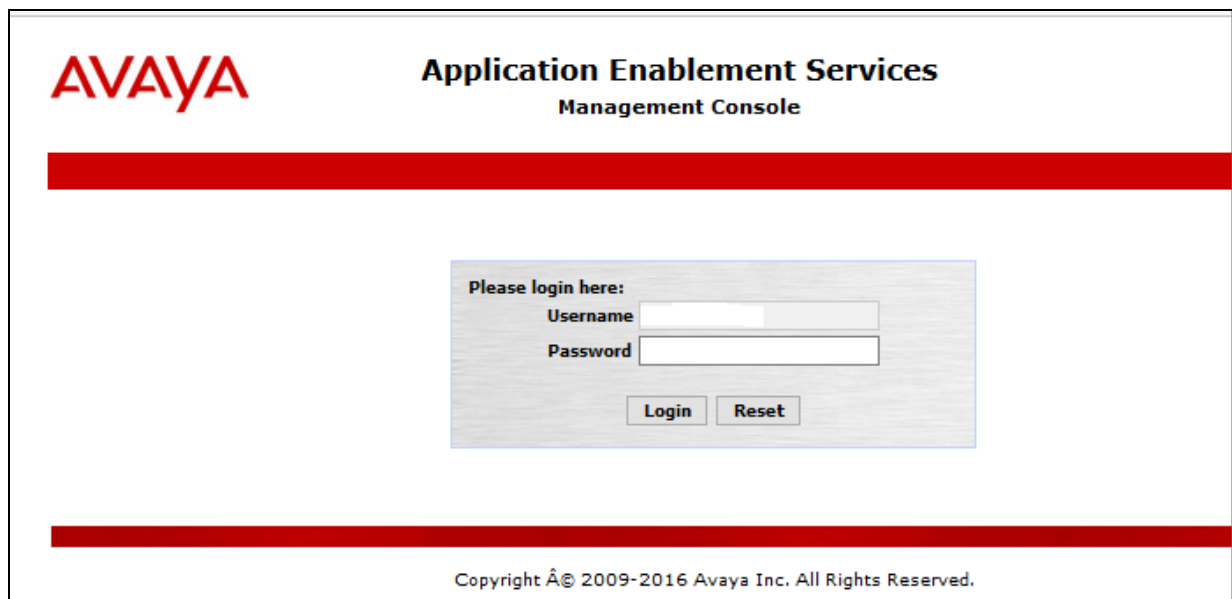
This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer Switch Connection
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer Envision user
- Administer CTI User permissions
- Enable DMCC and TSAPI Service port

6.1. Launch OAM Interface

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

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



The 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 thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" at the top, followed by "Username" and "Password" labels next to input fields. Below the input fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located at the bottom of the page, just above the footer text. The footer text at the very bottom reads "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console. At the top right, system information is displayed: Welcome: User devconnect, Last login: Thu Oct 27 16:34:31 2016 from 192.168.100.18, Number of prior failed login attempts: 0, HostName/IP: aes7x/10.1.10.70, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 7.0.1.0.3.15-0, Server Date and Time: Thu Oct 27 16:46:51 SGT 2016, HA Status: Not Configured. Below this is a red navigation bar with 'Home' on the left and 'Home | Help | Logout' on the right. A left sidebar contains a list of menu items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Welcome to OAM' and contains a detailed introduction to the OAM web interface, listing various administrative domains and their functions. At the bottom, a copyright notice states 'Copyright © 2009-2016 Avaya Inc. All Rights Reserved.'

6.2. Verify License

Select **Licensing → WebLM Server Access** from the left pane of the home screen and **Avaya WebLM** screen pops up (not shown). Click on the **License Administration** and the **Web License Manager** screen is displayed below.

The screenshot shows the Avaya Web License Manager login screen. It features the Avaya logo and the text 'Web License Manager' at the top. Below this is a red horizontal bar. The login form consists of two input fields: 'User Name:' and 'Password:'. To the right of the 'Password:' field are two buttons: 'Log On' and 'Clear'. At the bottom, a copyright notice states '© 2015 Avaya Inc. All Rights Reserved.'

Log in with the appropriate credentials.

Select **Licensed products** → **APPL_ENAB** → **Application Enablement** in the left pane to display the **Licensed Features** screen in the right pane. Scroll down the screen, and verify that there are sufficient licenses for **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below.

Web License Manager (WebLM v7.0)

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

WebLM Home
Install license
Licensed products
APPL_ENAB
Application Enablement
View license capacity
View peak usage
MSR
Media_Server
VSS
Voice_Portals
Uninstall license
Server properties
Manage users
Shortcuts
Help for Installed Product

Application Enablement (CTI) - Release: 7 - SID: 10503000
Standard License file

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: June 27, 2016 3:52:50 PM +08:00

License File Host IDs: VC-AF-73-9B-B4-D1

Licensed Features

13 Items
Show
All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	2500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	10
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	2500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	10
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	1
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	2500
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16

6.3. Administer Switch Connection

From the Home menu, select **Communication Manager Interface** → **Switch Connections**. Enter a descriptive name for the switch connection and click **Add Connection**. In this configuration, **Duplex** is used.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message. The main content area is titled 'Communication Manager Interface | Switch Connections'. On the left, a sidebar menu shows 'AE Services' expanded, with 'Communication Manager Interface' and 'Switch Connections' selected. The main panel displays a form for adding a new switch connection. The 'Connection Name' field contains the text 'Duplex'. The 'Add Connection' button is highlighted with a red box. Below the form, a table header is visible with columns: 'Connection Name', 'Processor Ethernet', 'Msg Period', and 'Number of Active Connections'.

The **Connection Details – Duplex** screen is displayed. For the **Switch Password** and **Confirm Switch Password** fields, enter the password that was administered in Communication Manager using the IP Services form in **Section 5.3**. Here we are using the **Processor Ethernet** as well for connection and the field needs to be checked. Click on **Apply** to effect changes.

The screenshot shows the 'Connection Details - Duplex' screen in the Avaya Application Enablement Services Management Console. The top navigation bar and sidebar menu are the same as in the previous screenshot. The main panel displays the 'Connection Details - Duplex' form. The 'Switch Password' and 'Confirm Switch Password' fields are highlighted with a red box. The 'Msg Period' is set to 30 minutes. The 'Provide AE Services certificate to switch' checkbox is unchecked. The 'Secure H323 Connection' checkbox is unchecked. The 'Processor Ethernet' checkbox is checked. The 'Apply' button is highlighted with a red box. The footer of the page reads 'Copyright © 2009-2016 Avaya Inc. All Rights Reserved.'

The Switch Connections screen is displayed. Select the newly added switch connection name and click **Edit PE/CLAN IPs**.

Application Enablement Services Management Console

Welcome: User devconnect
 Last login: Fri Oct 28 11:02:28 2016 from 192.168.100.18
 Number of prior failed login attempts: 0
 HostName/IP: aes7x/10.1.10.70
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.1.0.3.15-0
 Server Date and Time: Fri Oct 28 14:19:41 SGT 2016
 HA Status: Not Configured

Communication Manager Interface | Switch Connections
 Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
Duplex	Yes	30	1

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

In the **Edit Processor Ethernet IP – Duplex** screen, enter the host name or IP address of the PE/C-LAN used for AES connectivity. In this case, **10.1.10.230** is used, which corresponds to the **procr** address of the Communication Manager. Click **Add/Edit Name or IP**

Application Enablement Services Management Console

Welcome: User devconnect
 Last login: Fri Oct 28 11:02:28 2016 from 192.168.100.18
 Number of prior failed login attempts: 0
 HostName/IP: aes7x/10.1.10.70
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.1.0.3.15-0
 Server Date and Time: Fri Oct 28 14:26:44 SGT 2016
 HA Status: Not Configured

Communication Manager Interface | Switch Connections
 Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan

Edit Processor Ethernet IP - Duplex

Add/Edit Name or IP

Name or IP Address	Status
--------------------	--------

6.4. Administer TSAPI Link

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "devconnect". The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen with a table header containing "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the header are buttons for "Add Link", "Edit Link", and "Delete Link". The "Add Link" button is highlighted with a red box.

In the **Add TSAPI Links** screen, select the following values:

- **Link:** Select an available Link number from 1 to 16.
- **Switch Connection:** Administered switch connection in **Section 5.3**.
- **Switch CTI Link Number:** Corresponding CTI link number in **Section 5.3**.
- **ASAI Link Version:** Set to **7** for the latest version.
- **Security:** Select **Both** to allow for encrypted or unencrypted link.

Click **Apply Changes**.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form with fields for "Link", "Switch Connection", "Switch CTI Link Number", "ASAI Link Version", and "Security". Each field has a dropdown menu. The "Link" dropdown is set to "3", "Switch Connection" is set to "Duplex", "Switch CTI Link Number" is set to "3", "ASAI Link Version" is set to "7", and "Security" is set to "Both". The "Apply Changes" button is highlighted with a red box.

6.5. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case **Duplex**, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Switch Connections' selected under 'Communication Manager Interface'. The main area displays a table of switch connections. The 'Duplex' connection is selected with a radio button. Below the table, the 'Edit H.323 Gatekeeper' button is highlighted with a red box.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> Duplex	Yes	30	1

Buttons below the table: Edit Connection, Edit PE/CLAN IPs, **Edit H.323 Gatekeeper**, Delete Connection, Survivability Hierarchy

The **Edit H.323 Gatekeeper – Duplex** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper, in this case the Processor C-LAN is used as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - Duplex' screen. A text input field contains '10.1.10.230'. The 'Add Name or IP' button is highlighted with a red box. Below the input field is a 'Delete IP' button.

10.1.10.230 **Add Name or IP**

Name or IP Address

Delete IP

6.6. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Clear the **Enable SDB for DMCC Service** and **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** if they are checked, and click **Apply Changes**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Control' selected. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services', both of which are unchecked. Below the checkboxes is an 'Apply Changes' button. The top right corner displays system information: 'Welcome: User devconnect', 'Last login: Fri Oct 28 11:02:28 2016 from 192.168.100.18', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7x/10.1.10.70', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.1.0.3.15-0', 'Server Date and Time: Fri Oct 28 14:55:01 SGT 2016', and 'HA Status: Not Configured'. The top navigation bar shows 'Security | Security Database | Control' and 'Home | Help | Logout'.

6.7. Restart TSAPI Service

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Maintenance' expanded, with 'Service Controller' selected. The main content area is titled 'Service Controller'. It contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services: ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, Transport Layer Service, and TSAPI Service. The 'DMCC Service' and 'TSAPI Service' rows have checkboxes that are checked. Below the table is a link 'For status on actual services, please use [Status and Control](#)'. At the bottom, there is a row of buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The 'Restart Service' button is highlighted with a red box. The top right corner displays system information: 'Welcome: User devconnect', 'Last login: Fri Oct 28 11:02:28 2016 from 192.168.100.18', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7x/10.1.10.70', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.1.0.3.15-0', 'Server Date and Time: Fri Oct 28 14:56:50 SGT 2016', and 'HA Status: Not Configured'. The top navigation bar shows 'Maintenance | Service Controller' and 'Home | Help | Logout'.

6.8. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service.

Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Envision Click2Coach.

In this case, the associated unencrypted Tlink name is **AVAYA#DUPLEX#CSTA#AES7X**, which is automatically assigned by the Avaya AES server. Note the use of the switch connection **Duplex** from **Section 5.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "devconnect" with login details. A red navigation bar contains "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar shows a tree view with categories like "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", and "Security". Under "Security", the "Security Database" is expanded, showing "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks". The main content area, titled "Tlinks", lists two entries: "AVAYA#DUPLEX#CSTA#AES7X" (selected with a radio button and highlighted by a red box) and "AVAYA#DUPLEX#CSTA-S#AES7X". A "Delete Tlink" button is located below the list.

6.9. Administer Envision User

Select **User Management** → **User Admin** → **Add User** from the left pane to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: Welcome: User devconnect, Last login: Fri Oct 28 10:46:35 2016 from 192.168.100.18, Number of prior failed login attempts: 0, HostName/IP: aes7x/10.1.10.70, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 7.0.1.0.3.15-0, Server Date and Time: Fri Oct 28 11:05:05 SGT 2016, HA Status: Not Configured.

The main navigation bar includes 'User Management | User Admin | Add User' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'User Management' expanded, and 'User Admin' selected, leading to the 'Add User' option.

The 'Add User' form contains the following fields:

- * User Id: Envision
- * Common Name: Envision
- * Surname: Envision
- * User Password: [Empty]
- * Confirm Password: [Empty]
- Admin Note: [Empty]
- Avaya Role: None
- Business Category: [Empty]
- Car License: [Empty]
- CM Home: [Empty]
- Css Home: [Empty]
- CT User: Yes
- Department Number: [Empty]
- Display Name: [Empty]

Fields marked with * can not be empty.

6.10. Administer CTI User Permissions

Select **Security** → **Security Database** → **CTI Users** → **List All Users** from the AES Management Console Home menu. Select the User ID created in **Section 5.9** and click **Edit**.

AVAYA

Application Enablement Services
Management Console

Welcome: User devconnect
Last login: Wed Nov 2 16:43:59 2016 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Nov 02 16:59:42 SGT 2016
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Audit

Certificate Management

Enterprise Directory

Host AA

Security Database

Control

CTI Users

List All Users

Search Users

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> CRTADM	AMC	NONE	NONE
<input type="radio"/> Cyara	Cyara	NONE	NONE
<input checked="" type="radio"/> Envision	Envision	NONE	NONE
<input type="radio"/> devconnect	devconnect	NONE	NONE
<input type="radio"/> psadmin	psadmin	NONE	NONE

Check the **Unrestricted Access** box. Click **Apply Changes**.

AVAYA

Application Enablement Services
Management Console

Welcome: User devconnect
Last login: Wed Nov 2 16:43:56 2016 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Nov 02 16:55:41 SGT 2016
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Audit

Certificate Management

Enterprise Directory

Host AA

Security Database

Control

CTI Users

List All Users

Search Users

Edit CTI User

User Profile:

User IDCommon NameWorktop NameUnrestricted Access

EnvisionEnvisionNONE☒

Call and Device Control:

Call Origination/Termination and Device StatusNone

Call and Device Monitoring:

Device MonitoringNone

Calls On A Device MonitoringNone

Call Monitoring☐

Routing Control:

Allow Routing on Listed DevicesNone

6.11. Enable DMCC and TSAPI Service Port

Select **Networking** → **Ports** from the left pane to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Do the same for **TSAPI Ports** under the **Enabled** column.

AVAYA

Application Enablement Services
Management Console

Welcome: User devconnect
Last login: Fri Oct 28 11:02:28 2016 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Oct 28 14:41:00 SGT 2016
HA Status: Not Configured

Networking | PortsHome | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

Security

Status

User Management

Utilities

Help

Ports

CVLAN Ports

Unencrypted TCP Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

7. Configure Envision Click2Coach

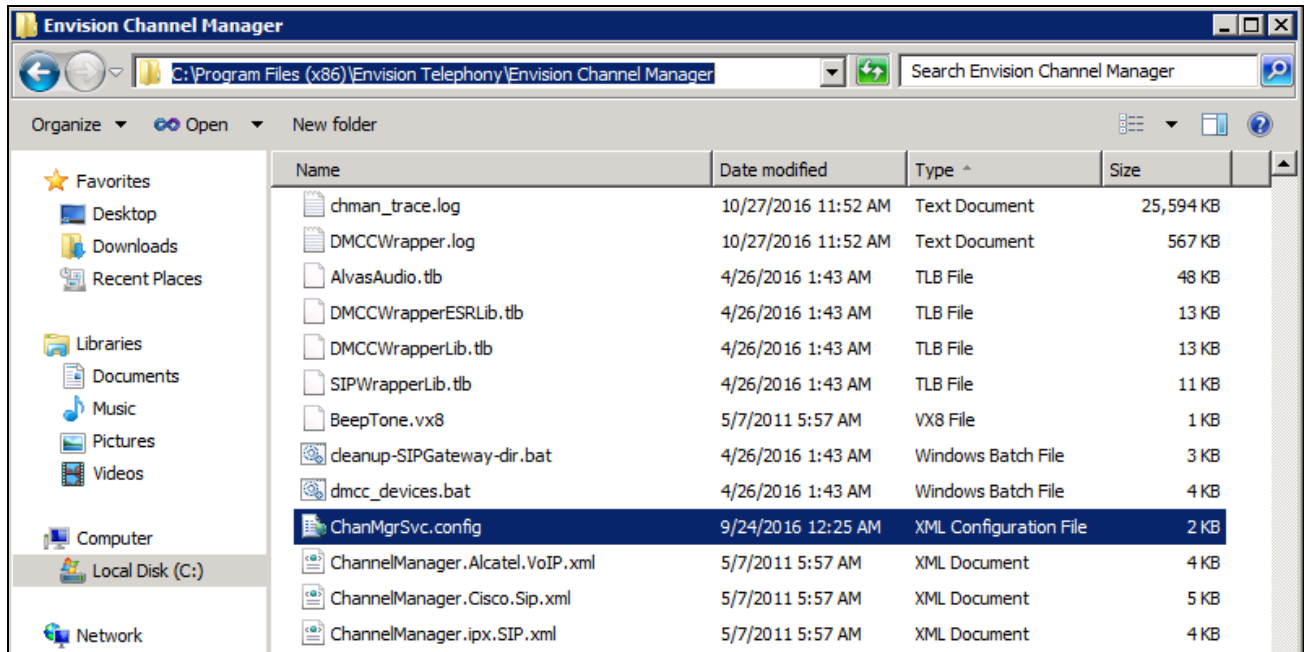
This section provides the procedures for configuring Envision Click2Coach. The procedures include the following areas:

- Administer ChanMgrSvc.config
- Administer ChannelManager.xml
- Launch Administrator
- Administer System Settings
- Administer Telephony settings
- Administer Telephony TSAPI
- Administer Telephony Envision servers
- Administer Telephony device IDs
- Administer Telephony ACD IDs
- Administer Users
- Restart Services
- Administer Channels

The configuration of Click2Coach is performed by Envision Professional Services engineers. The procedural steps are presented in these Application Notes for informational purposes. These Application Notes assume that the configurations of a site, server, PBX, and storage volumes are all in place and will not be covered.

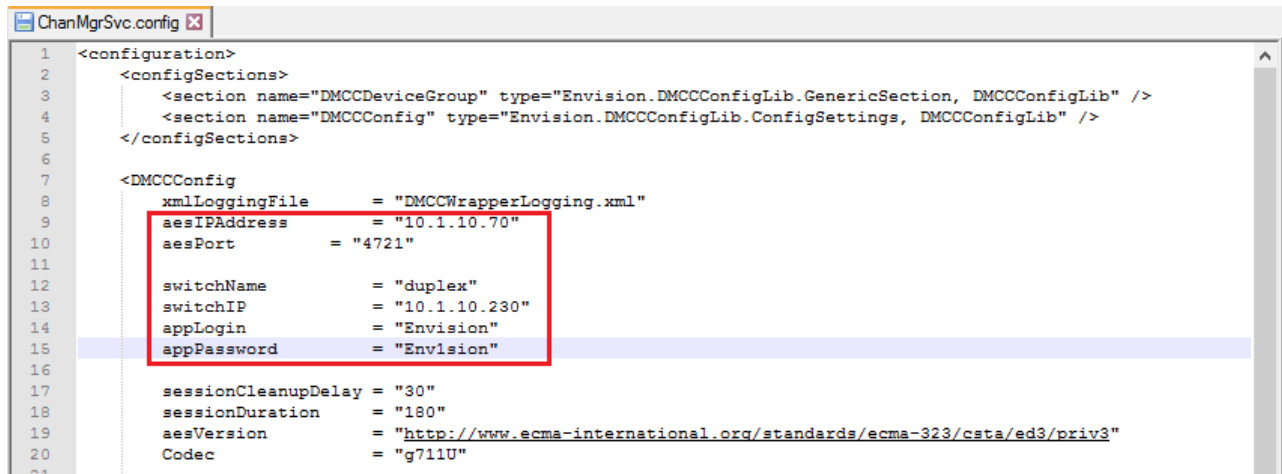
7.1. Administer ChanMgrSvc.config

From the Click2Coach server, navigate to the **C:\Program Files (x86)\Envision Telephony\Envision Channel Manager** directory to locate the **ChanMgrSvc.config** file shown below.



Open the **ChanMgrSvc.config** file with a text editor application such as Notepad++. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **aesIPAddress:** IP address of the AES server.
- **aesPort:** DMCC unencrypted port number from **Section 6.11**.
- **switchName:** Switch connection name from **Section 6.3**.
- **switchIP:** IP address of the H.323 gatekeeper from **Section 6.5**.
- **appLogin:** Envion user credentials from **Section 6.9**.
- **appPassword:** Envion user credentials from **Section 6.9**.



```

1 <configuration>
2   <configSections>
3     <section name="DMCCDeviceGroup" type="Envion.DMCCConfigLib.GenericSection, DMCCConfigLib" />
4     <section name="DMCCConfig" type="Envion.DMCCConfigLib.ConfigSettings, DMCCConfigLib" />
5   </configSections>
6
7   <DMCCConfig
8     xmlLoggingFile      = "DMCCWrapperLogging.xml"
9     aesIPAddress        = "10.1.10.70"
10    aesPort              = "4721"
11
12    switchName           = "duplex"
13    switchIP             = "10.1.10.230"
14    appLogin             = "Envion"
15    appPassword          = "Envion"
16
17    sessionCleanupDelay  = "30"
18    sessionDuration      = "180"
19    aesVersion            = "http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv3"
20    Codec                = "g711U"
21  >

```

Scroll to the bottom of the screen. For **rtpIPAddress**, enter the IP address of the Envion server. In the **DMCCDeviceGroup** section, create an entry line with the extension and password for each virtual IP softphone from **Section 5.6**, as shown below.



```

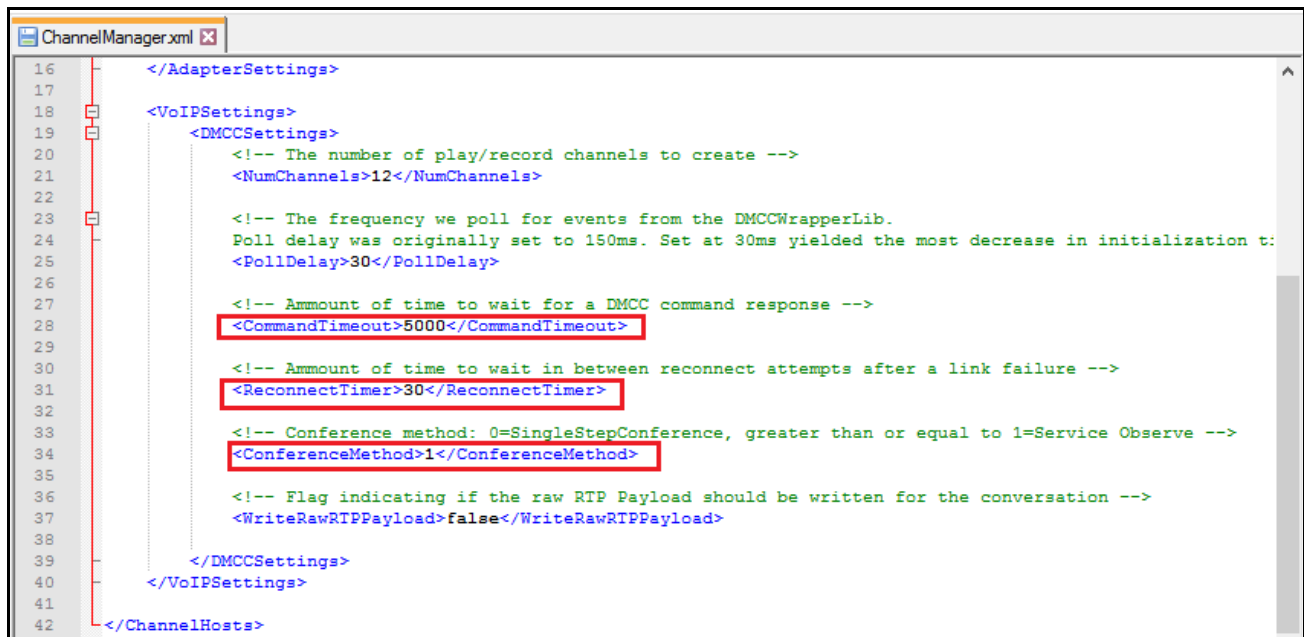
26 beepToneFile          = "c:\temp\BeepTone.vx8"
27 beepToneFreq         = "440"
28 beepToneGain         = "1.0"
29
30 rtpIPAddress          = "10.1.10.124"
31 rtpPortBase          = "18000"
32
33 gcTimer               = "0"
34 bridgedDeviceList     = ""
35 </>
36
37 <!-- 3.0 aesVersion = "3.0" -->
38 <!-- 3.1 aesVersion = "http://www.ecma-international.org/standards/ecma-323/csta/ed2/priv1"
39 <!-- 4.0 aesVersion = "http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv1"
40 <!-- 4.1 aesVersion = "http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv2"
41 <!-- 4.2 aesVersion = "http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv3"
42
43
44 <DMCCDeviceGroup name="Avaya DMCC Devices">
45   <Device channel="0" extension="19901" password="19901"/>
46   <Device channel="1" extension="19902" password="19902"/>
47   <Device channel="2" extension="19903" password="19903"/>
48   <Device channel="3" extension="19904" password="19904"/>
49   <Device channel="4" extension="19905" password="19905"/>
50 </DMCCDeviceGroup>
51
52 </configuration>

```

7.2. Administer ChannelManager.xml

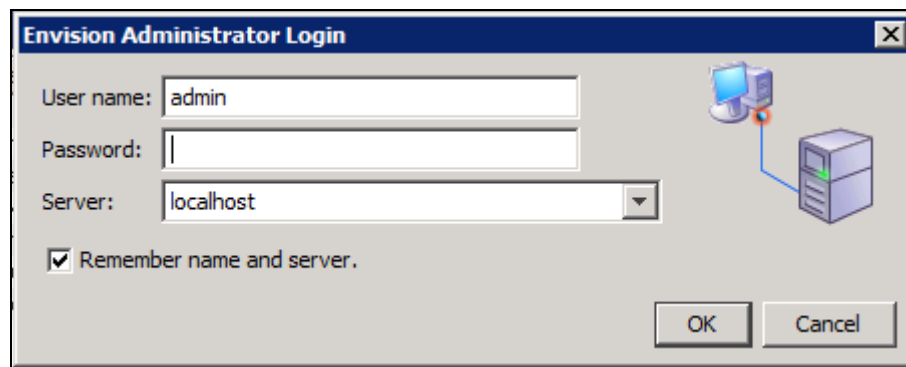
From the same **C:\Program Files\Envision Telephony\Envision Server\ChannelManager** directory, open the **ChannelManager.xml** file.

Scroll down to the **DMCCSettings** section. For **ReconnectTimer**, enter **30**. For **ConferenceMethod**, enter **1** to enable Service Observing. The **CommandTimeout** is set at **5000** (msecs) to wait for AES respond for any request.

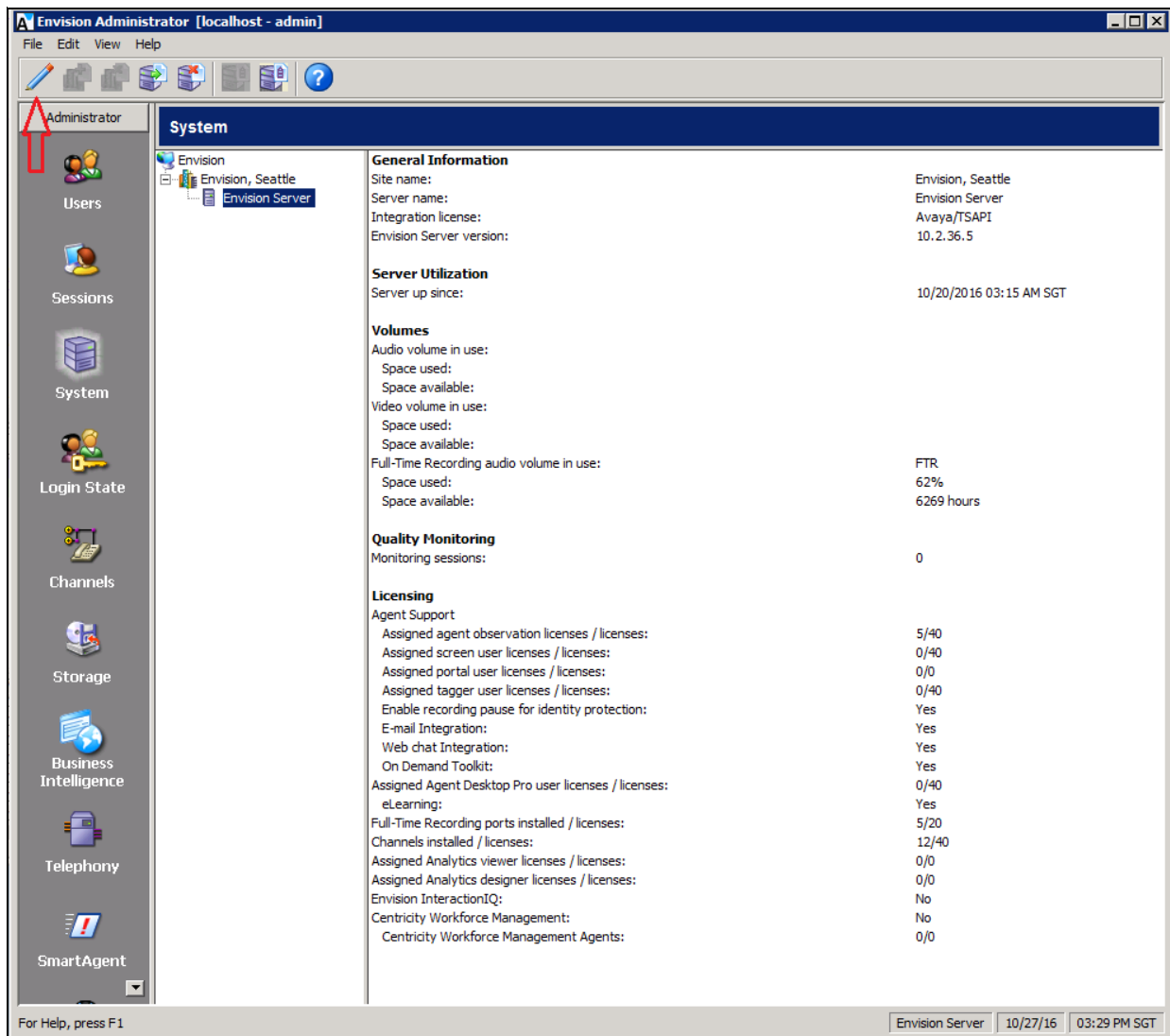


7.3. Launch Administrator

From the Envision server, select **Start → All Programs → Envision Telephony → Envision Server Suite → Administrator** to launch the Administrator application. The **Envision Administrator Login** screen is displayed. Log in using the appropriate credentials such as admin.



The **Envision Administrator** screen is displayed, and the right pane defaults to the **System** screen. Click on the **Edit system settings**  icon.



Envision Administrator [localhost - admin]

File Edit View Help

Administrator

System

Envision

- Envision, Seattle
 - Envision Server

General Information

Site name:	Envision, Seattle
Server name:	Envision Server
Integration license:	Avaya/TSAPI
Envision Server version:	10.2.36.5

Server Utilization

Server up since:	10/20/2016 03:15 AM SGT
------------------	-------------------------

Volumes

Audio volume in use:	
Space used:	
Space available:	
Video volume in use:	
Space used:	
Space available:	
Full-Time Recording audio volume in use:	FTR
Space used:	62%
Space available:	6269 hours

Quality Monitoring

Monitoring sessions:	0
----------------------	---

Licensing

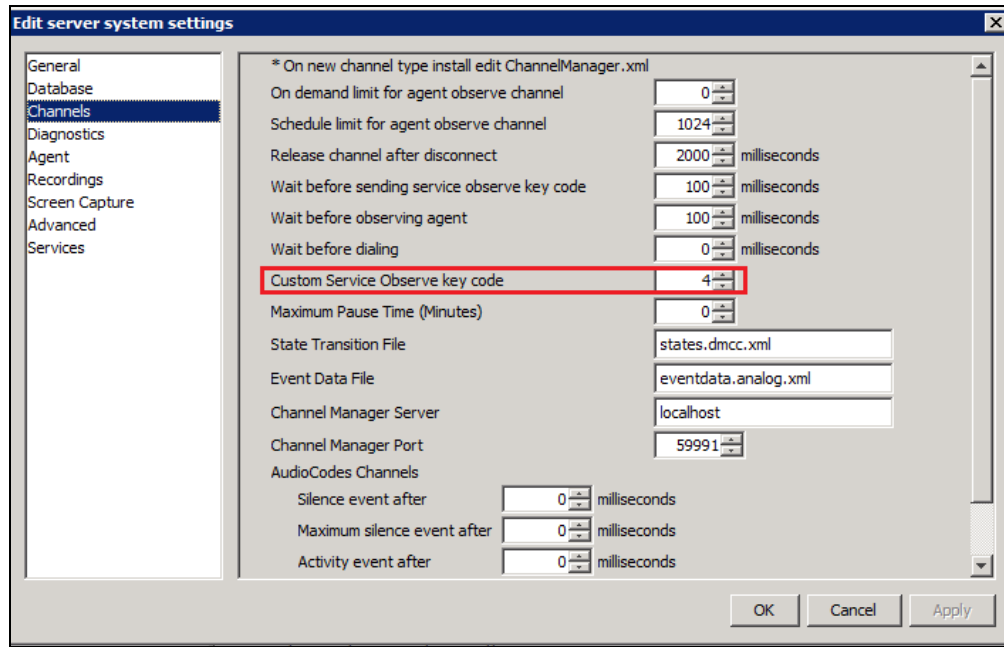
Agent Support	
Assigned agent observation licenses / licenses:	5/40
Assigned screen user licenses / licenses:	0/40
Assigned portal user licenses / licenses:	0/0
Assigned tagger user licenses / licenses:	0/40
Enable recording pause for identity protection:	Yes
E-mail Integration:	Yes
Web chat Integration:	Yes
On Demand Toolkit:	Yes
Assigned Agent Desktop Pro user licenses / licenses:	0/40
eLearning:	Yes
Full-Time Recording ports installed / licenses:	5/20
Channels installed / licenses:	12/40
Assigned Analytics viewer licenses / licenses:	0/0
Assigned Analytics designer licenses / licenses:	0/0
Envision InteractionIQ:	No
Centricity Workforce Management:	No
Centricity Workforce Management Agents:	0/0

For Help, press F1

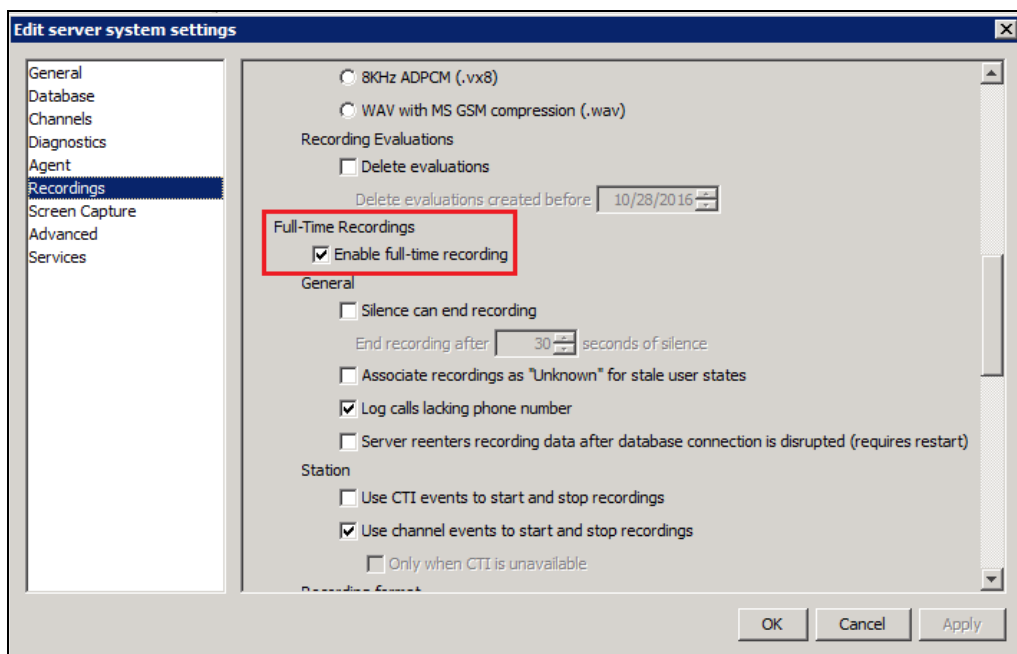
Envision Server 10/27/16 03:29 PM SGT

7.4. Administer System Settings

The **Edit server system settings** screen is displayed. Select **Channels** from the left pane. For **Custom Service Observe key code**, select the button number associated with the Service Observing feature on the virtual IP softphones from **Section 5.6**.



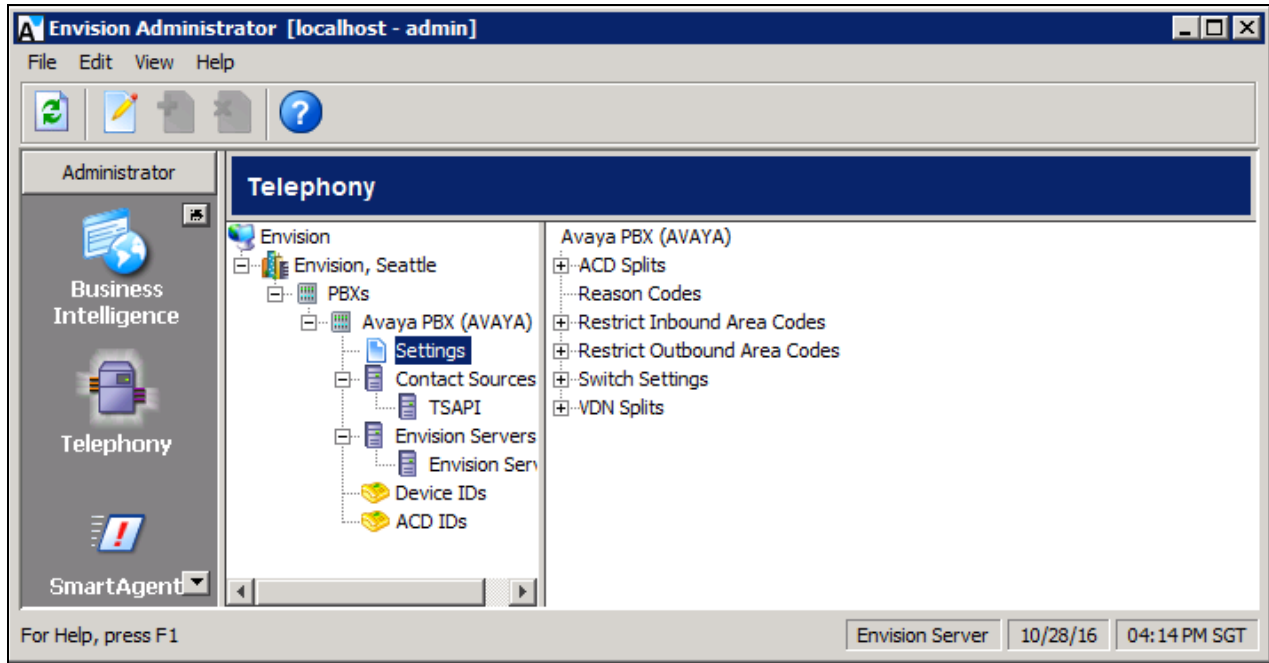
Select **Recordings** from the left pane, and scroll the screen down to the **Full-Time Recordings** section. Check **Enable full-time recording**, as shown below. Click **OK** to complete.



7.5. Administer Telephony Settings

The **Envision Administrator** screen is displayed again. Scroll down the left pane as necessary and select **Telephony** to display the **Telephony** screen in the right pane.

Double click on **Envision → Envision, Seattle → PBXs → Avaya PBX (AVAYA) → Settings** in the middle pane, where **Envision, Seattle** is the pre-configured site name and **Avaya PBX (AVAYA)** is the pre-configured PBX name. Note that the names may vary.



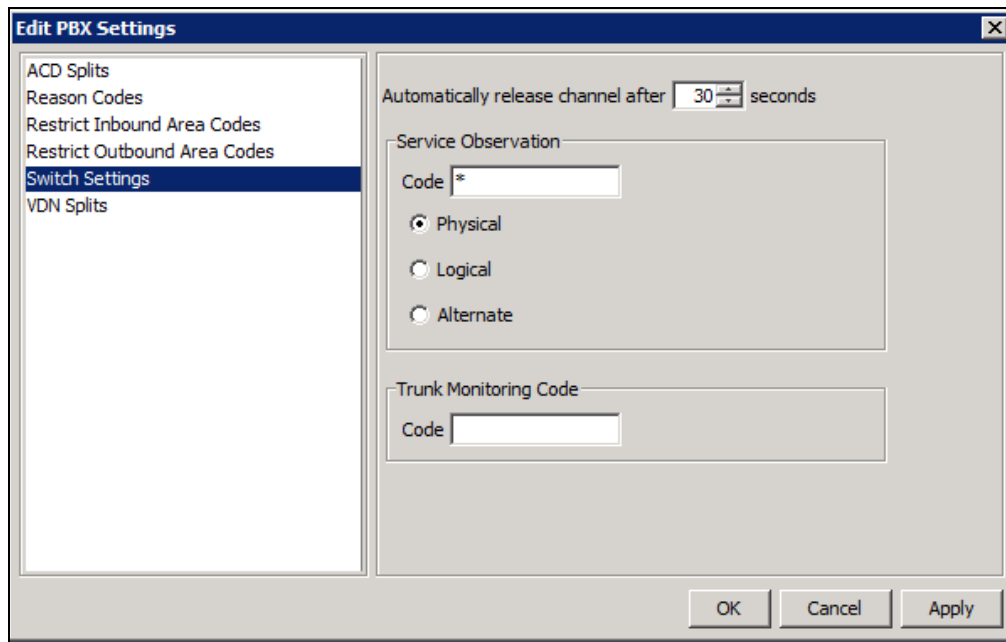
The **Edit PBX Settings** screen is displayed. Select **ACD Splits** from the left pane. Enter **13001** for the Hunt Group in **Section 2**.

The screenshot shows the 'Edit PBX Settings' dialog box. On the left, a list of settings includes 'ACD Splits', 'Reason Codes', 'Restrict Inbound Area Codes', 'Restrict Outbound Area Codes', 'Switch Settings', and 'VDN Splits'. 'ACD Splits' is selected. The main area on the right has a header 'ACD Split' and a text input field containing '13001'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Select **VDN Splits** on the left pane. Enter **14001** for the VDN in **Section 2**.

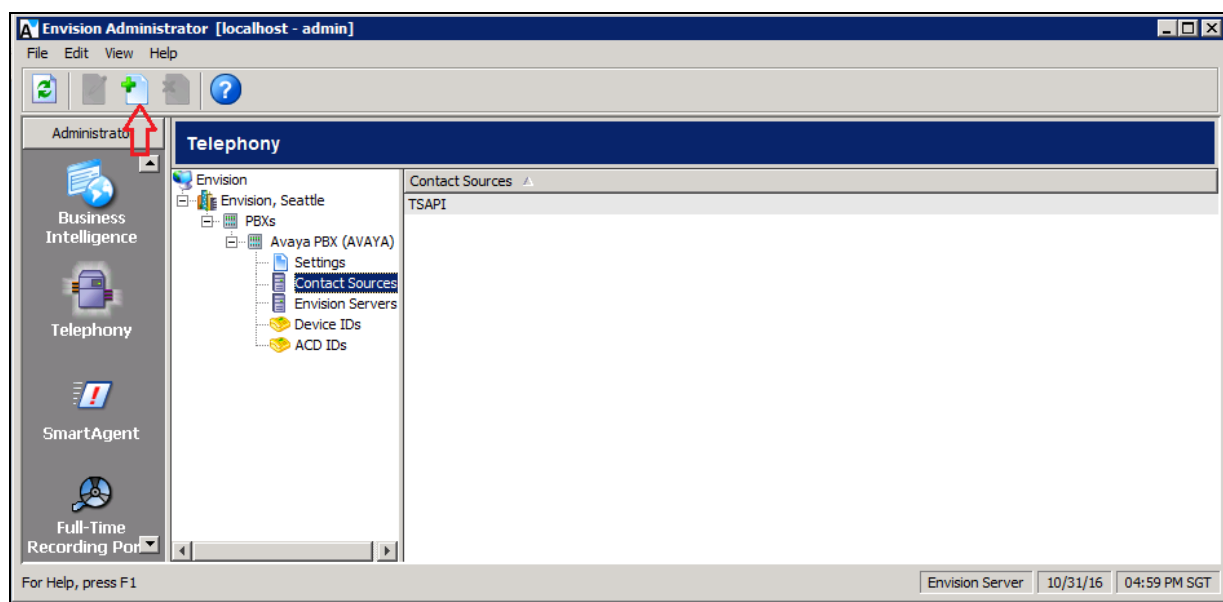
The screenshot shows the 'Edit PBX Settings' dialog box. On the left, the same list of settings is shown, but 'VDN Splits' is now selected. The main area on the right has a header 'VDN Split' and a text input field containing '14001'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Select **Switch Settings** on the left pane. For **Code** under **Service Observation**, enter a non-blank value to denote this method being used. * is used as a arbitrary value here. Retain the default values in the remaining fields.



7.6. Administer Telephony TSAPI

The **Telephony** screen is displayed again. Select **Envision** → **Envision, Seattle** → **PBXs** → **Avaya PBX (AVAYA)** → **Contact Sources** in the middle pane, and click the **New telephony setting** icon shown below.



The **Add Contact Source** screen is displayed. Enter a descriptive **Name**. Select **TSAPI** as **Contact Source Type**, and click **Edit Settings**.

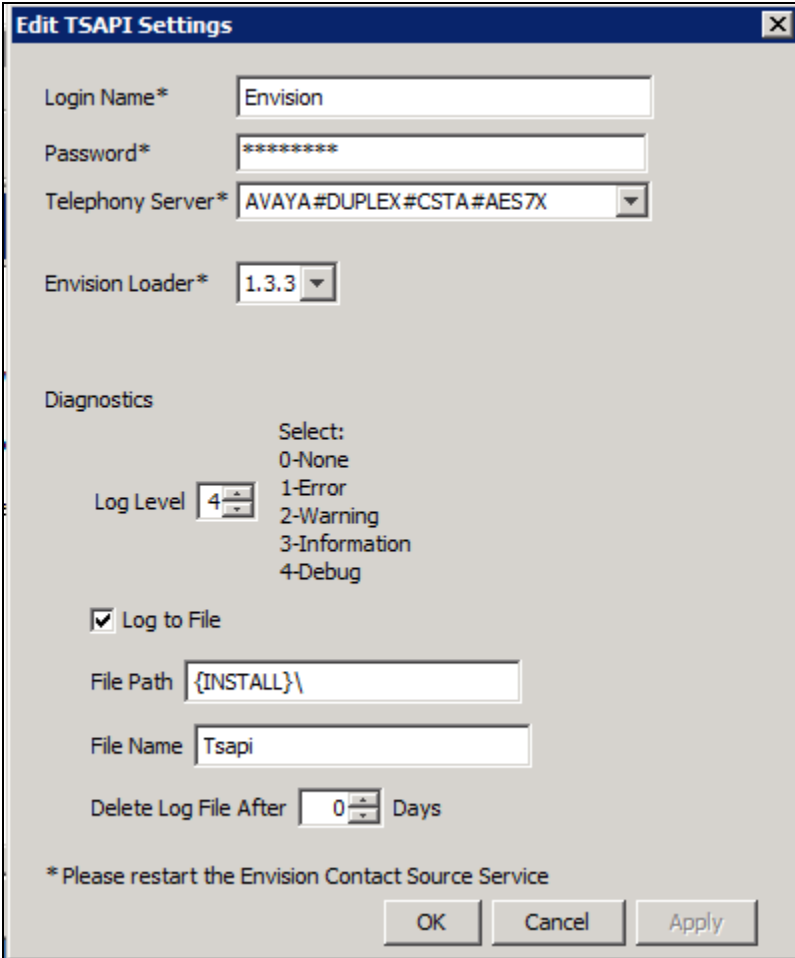


The image shows a Windows-style dialog box titled "Add Contact Source". It has a standard title bar with a close button (X). The dialog contains two main input areas: a text field labeled "Name" with the text "TSAPI" entered, and a list box labeled "Contact Source Type" with "TSAPI" selected and "Generic" listed below it. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Edit Settings...".

The **Edit TSAPI Settings** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Login Name:** Envision user credentials from **Section 6.9**.
- **Password:** Envision user credentials from **Section 6.9**.
- **Telephony Server:** The Tlink name from **Section 6.8**.
- **Envision Loader:** 1.3.3

Note that regardless of the value shown in the **Envision Loader** field, the actual version of the installed TSAPI client will be used. In the compliance testing, **Delete Log File After** was set to **0** days to keep the logs. Otherwise, the logs can be deleted for a specified number of days.

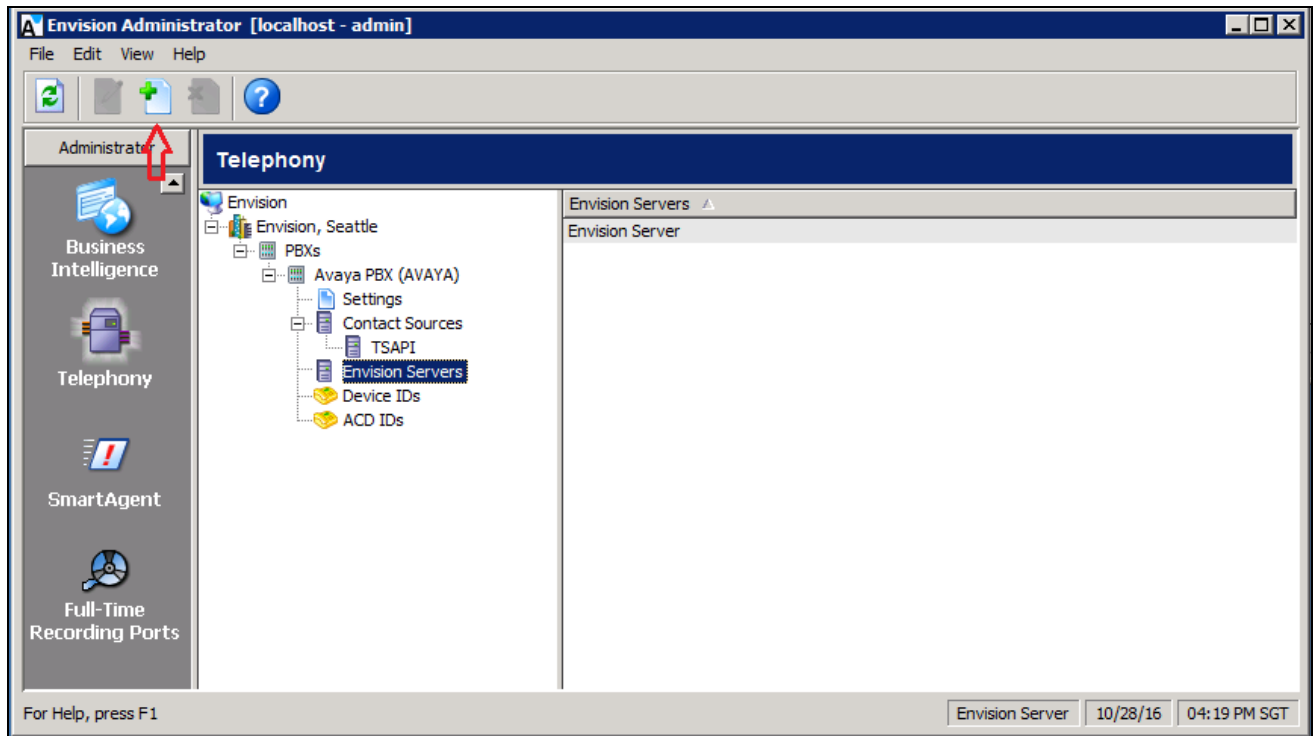


The screenshot shows the 'Edit TSAPI Settings' dialog box. It contains the following fields and options:

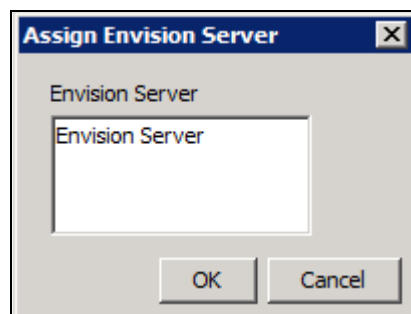
- Login Name*:** Text box containing 'Envision'.
- Password*:** Password box containing '*****'.
- Telephony Server*:** Dropdown menu showing 'AVAYA#DUPLEX#CSTA#AES7X'.
- Envision Loader*:** Dropdown menu showing '1.3.3'.
- Diagnostics:**
 - Log Level:** Spin box set to '4'. A list to the right shows options: 0-None, 1-Error, 2-Warning, 3-Information, 4-Debug.
 - Log to File:** Checked checkbox.
 - File Path:** Text box containing '{INSTALL}\'
 - File Name:** Text box containing 'Tsapi'.
 - Delete Log File After:** Spin box set to '0' followed by 'Days'.
- Footer:** A note '* Please restart the Envision Contact Source Service' and three buttons: 'OK', 'Cancel', and 'Apply'.

7.7. Administer Telephony Envision Servers

The **Telephony** screen is displayed again. Select the **Envision** → **Envision, Seattle** → **PBXs** → **Avaya PBX (AVAYA)** → **Envision Servers** in the middle pane, and click on the **New telephony setting** icon shown below.

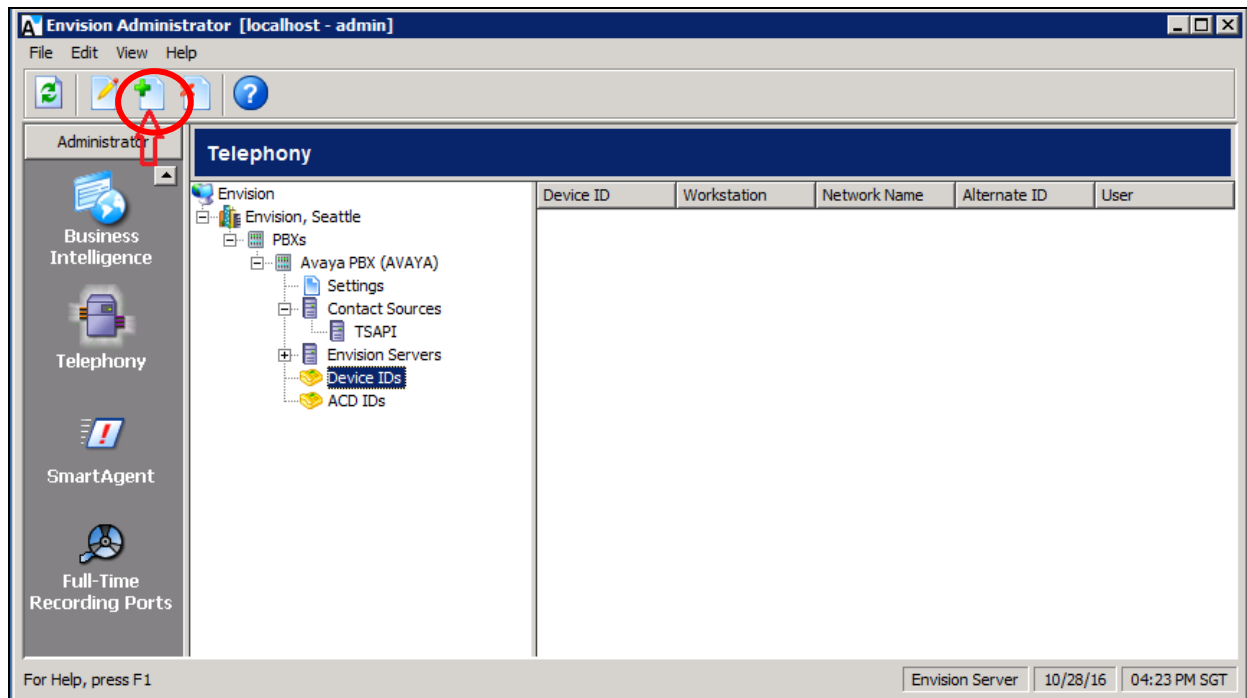


The **Assign Envision Server** screen is displayed. Select the proper **Envision Server**, as shown below.



7.8. Administer Telephony Device IDs

The **Telephony** screen is displayed again. Select **Envision** → **Envision, Seattle** → **PBXs** → **Avaya PBX (AVAYA)** → **Device IDs** in the middle pane, and click the **New telephony setting** icon shown below.



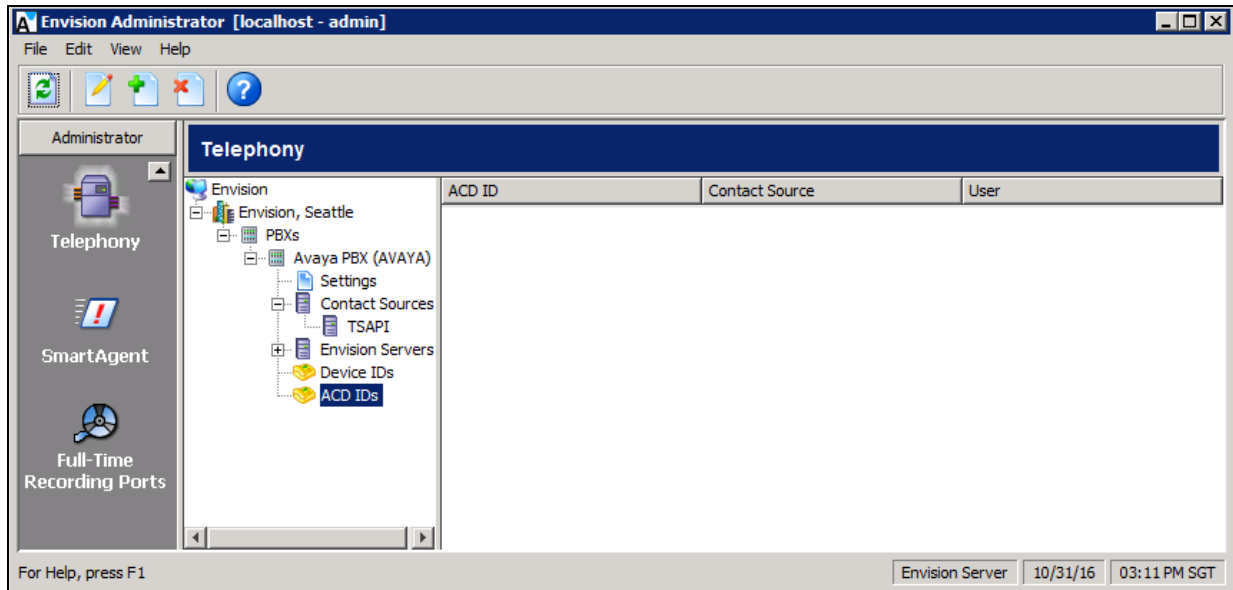
The **Add Device IDs** screen is displayed. Create a device ID for each agent station from **Section 2**. Note that ranges can be used for consecutive agent stations, as shown below.

The 'Add Device IDs' dialog box is shown. It has a title bar with 'Add Device IDs' and a close button. The dialog contains the following fields and controls:

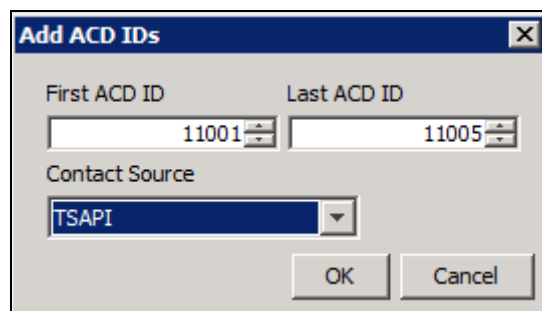
- First Device ID:** A text box with the value '10001'.
- Last Device ID:** A text box with the value '10005'.
- Workstation:** A text box.
- Network Name:** A text box.
- Alternate ID:** A checkbox that is currently unchecked.
- Bottom:** 'OK' and 'Cancel' buttons.

7.9. Administer Telephony ACD IDs

The **Telephony** screen is displayed again. Select **Envision** → **Envision, Seattle** → **PBXs** → **Avaya PBX (AVAYA)** → **ACD IDs** in the middle pane, and click the **New telephony setting** icon shown below.

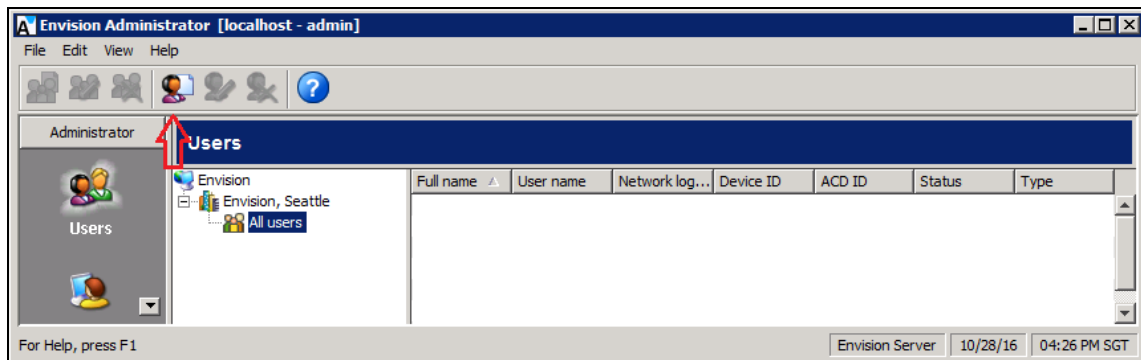


The **Add ACD IDs** screen is displayed. Create an ACD ID for each agent station from **Section 2**. Note that ranges can be used for consecutive agent stations, as shown below. Select **TSAPI** from the drop down menu as the **Contact Source**.



7.10. Administer Users

From the **Envision Administrator** screen, scroll the left pane as necessary and select **Users**. The **Users** screen is displayed in the right pane. Select **Envision** → **Envision, Seattle** → **All Users** in the middle pane, and click the **New user** icon shown below.



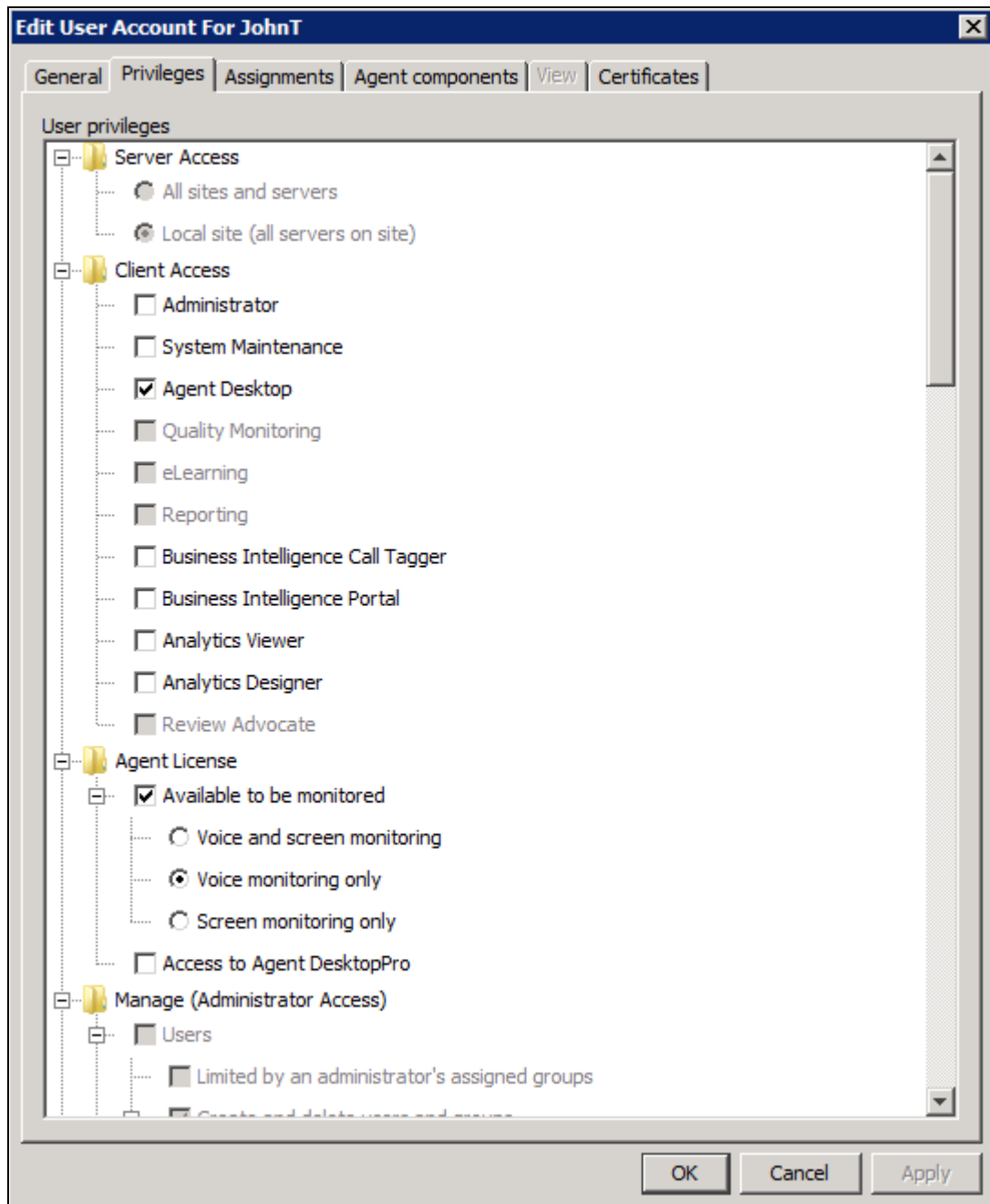
The **Create New User Account** screen is displayed. Create a user to correspond to the first agent in **Section 2**. Enter a desired **User name** and **Full name**. Select the proper **Device ID**, and retain the default values in the remaining fields. Below is a created user.

The 'Edit User Account For JohnT' dialog box is shown with the 'General' tab selected. The fields are as follows:

- Domain name: [Empty]
- Network login name: [Empty]
- User name *: JohnT
- Full name *: John Travel
- Change password...: [Button]
- * Required Field
- PBX: Avaya PBX
- Device ID: -
- ACD ID: [Empty]
- Account:
 - ☐ Inactive
 - ☒ Active
 - ☐ Active until: 10/31/2016

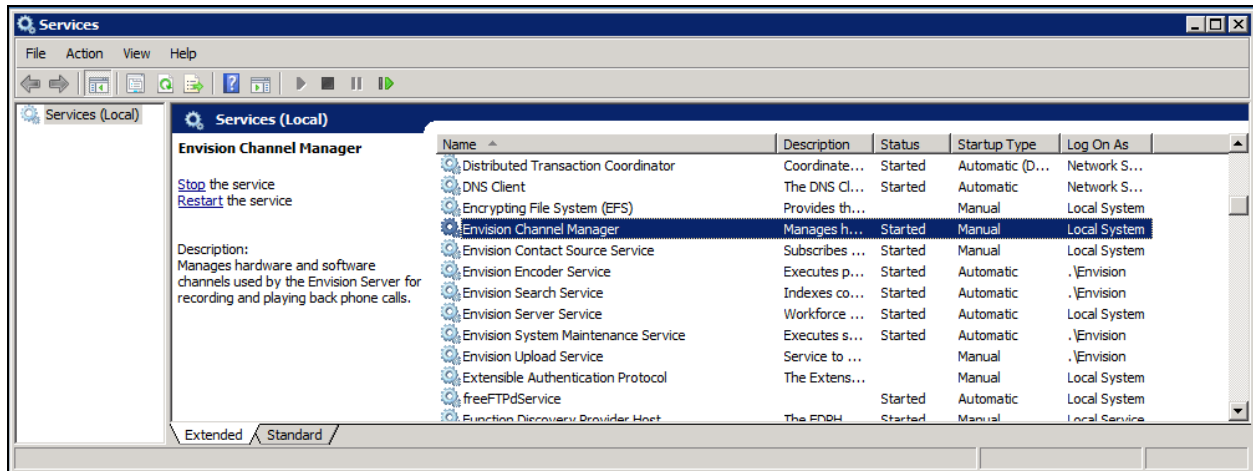
A calendar is displayed for the 'Active until' date, showing the month of October 2016. The calendar has a header row with days of the week (S, M, T, W, T, F, S) and a grid of dates from 1 to 31.

Select the **Privileges** tab, and check the desired privileges. The screenshot below shows the settings used for the agent. Repeat this section for all agents.



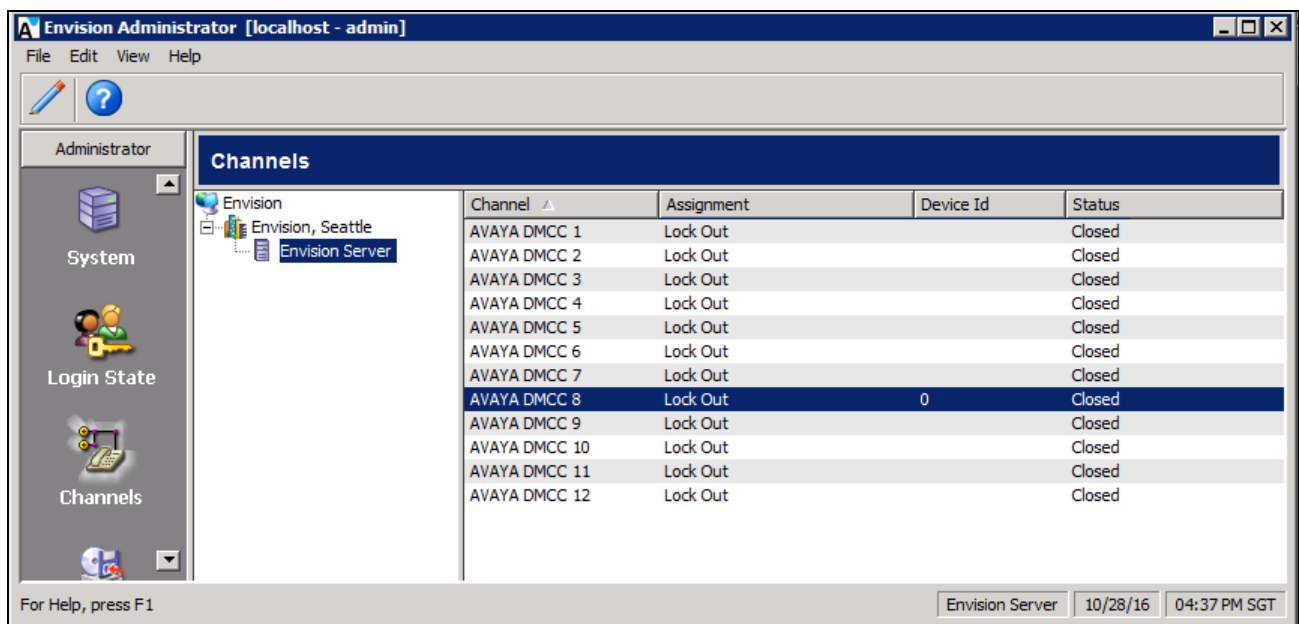
7.11. Restart Services

From the Envision server, select **Start → All Programs → Administrative Tools → Services** to display the **Services (Local)** screen. Restart the **Envision Channel Manager**, **Envision Contact Source Service**, and **Envision Server Service** shown below.

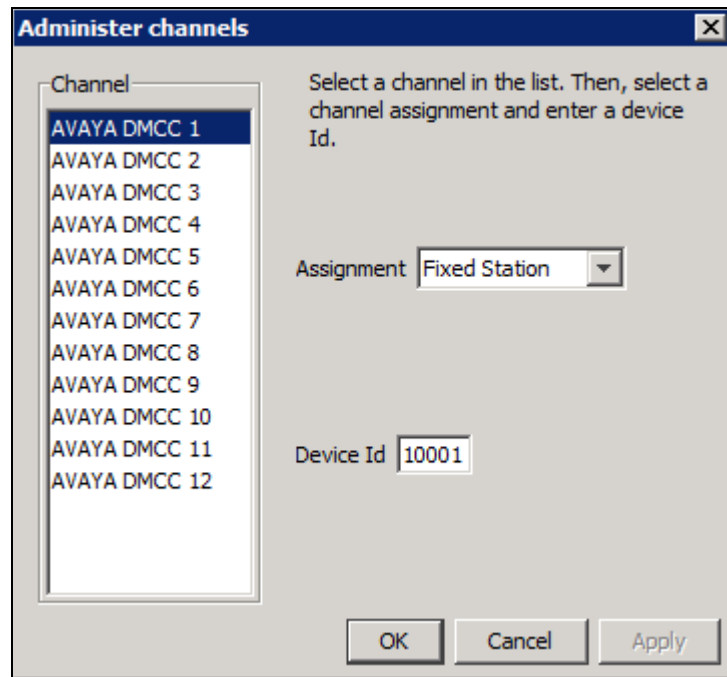


7.12. Administer Channels

From the **Envision Administrator** screen, scroll the left pane as necessary and select **Channels**. The **Channels** screen is displayed in the right pane. Double click on the first channel entry in the right pane.



The **Administer channels** screen is displayed. For **Assignment**, select **Fixed Station**. For **Device Id**, enter the first station extension from **Section 2**. Repeat this section for all 5 channels.



The image shows a Windows-style dialog box titled "Administer channels". On the left, there is a list box labeled "Channel" containing 12 items: "AVAYA DMCC 1" through "AVAYA DMCC 12". "AVAYA DMCC 1" is currently selected. To the right of the list box, there is instructional text: "Select a channel in the list. Then, select a channel assignment and enter a device Id." Below this text, there is a label "Assignment" followed by a dropdown menu showing "Fixed Station". Further down, there is a label "Device Id" followed by a text input field containing the number "10001". At the bottom right of the dialog box are three buttons: "OK", "Cancel", and "Apply".

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Envision Click2Coach.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is **established** for the CTI link number administered in **Section 5.3**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
3	7	no	aes7x	established	15	15

Verify the registration status of the virtual IP softphones by using the **list registered-ip-stations** command. Verify that the virtual IP softphones from **Section 5.6** are displayed, as shown below.

```
list registered-ip-stations ext 19901 count 5
```

REGISTERED IP STATIONS						
Station or Orig Port	Ext	Set Type/ Net Rgn	Prod ID/ Release	Skt	Station IP Address/ Gatekeeper IP Address	
19901		4624	IP_API_A	tcp	10.1.10.70	
		1	3.2040		10.1.10.230	
19902		4624	IP_API_A	tcp	10.1.10.70	
		1	3.2040		10.1.10.230	
19903		4624	IP_API_A	tcp	10.1.10.70	
		1	3.2040		10.1.10.230	
19904		4624	IP_API_A	tcp	10.1.10.70	
		1	3.2040		10.1.10.230	
19905		4624	IP_API_A	tcp	10.1.10.70	
		1	3.2040		10.1.10.230	

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the DMCC link by selecting **Status** → **Status and Control** → **DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed. On the lower portion of the screen, verify that the **User** column shows an active session with the Envision user name from **Section 6.9**, and that the **# of Associated Devices** column reflects the number of station extensions from **Section 2** plus the number of virtual softphones from **Section 5.6**.

AVAYA

Application Enablement Services
Management Console

Welcome: User devconnect
Last login: Fri Oct 28 15:30:59 2016 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Oct 28 16:44:45 SGT 2016
HA Status: Not Configured

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Fri Oct 28 16:43:50 SGT 2016

Service Uptime: 2 days, 1 hours 16 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 10

Number of Existing Devices: 10

Number of Devices Created Since Service Boot: 90

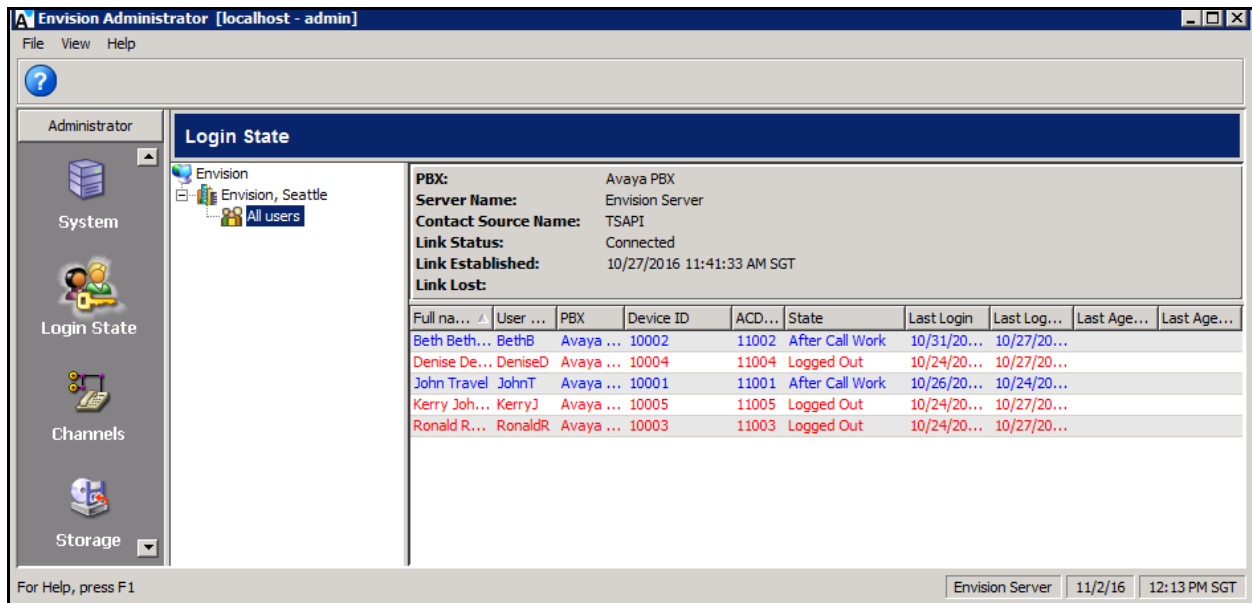
	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	BC38DD32E9B1398EA 31D12181E893213-9	Envision	duplex	10.1.10.124	XML Unencrypted	10

Terminate Sessions Show Terminated Sessions

Item 1-1 of 1
1 Go

8.3. Verify Envision Click2Coach

Log an agent into the Skill group to handle and complete an ACD call. From the **Envision Administrator** screen, scroll the left pane as necessary and select **Login State**. Select **Envision** → **Envision, Seattle** → **All Users** in the middle pane. Verify the agent's states.



Administrator

Login State

Envision
Envision, Seattle
All users

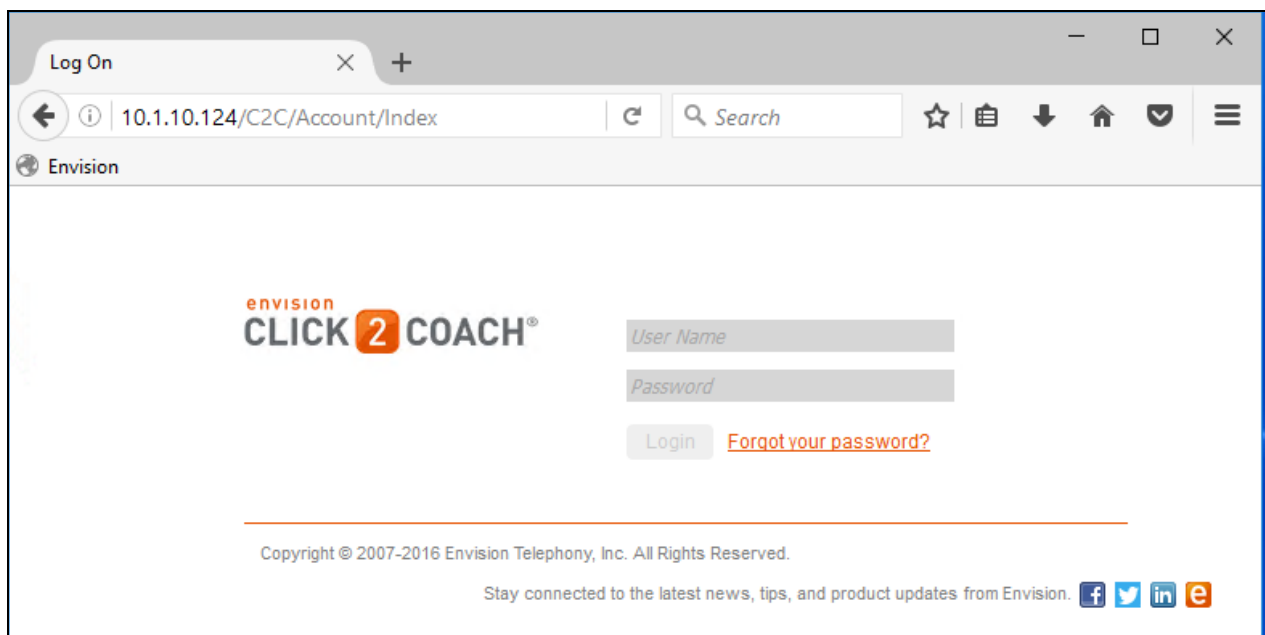
PBX: Avaya PBX
Server Name: Envision Server
Contact Source Name: TSAPI
Link Status: Connected
Link Established: 10/27/2016 11:41:33 AM SGT
Link Lost:

Full na...	User ...	PBX	Device ID	ACD...	State	Last Login	Last Log...	Last Age...	Last Age...
Beth Beth...	BethB	Avaya ...	10002	11002	After Call Work	10/31/20...	10/27/20...		
Denise De...	DeniseD	Avaya ...	10004	11004	Logged Out	10/24/20...	10/27/20...		
John Travel	JohnT	Avaya ...	10001	11001	After Call Work	10/26/20...	10/24/20...		
Kerry Joh...	KerryJ	Avaya ...	10005	11005	Logged Out	10/24/20...	10/27/20...		
Ronald R...	RonaldR	Avaya ...	10003	11003	Logged Out	10/24/20...	10/27/20...		

For Help, press F1

Envision Server 11/2/16 12:13 PM SGT

From the supervisor PC, access the Envision Click2Coach web-based interface by using the URL “http://ip-address/C2C/Account/Index” in an Internet browser window, where “ip-address” is the IP address of the Envision server. Log in with appropriate credentials.



Log On

10.1.10.124/C2C/Account/Index

Envision

envision
CLICK2 COACH®

User Name

Password

Login [Forgot your password?](#)

Copyright © 2007-2016 Envision Telephony, Inc. All Rights Reserved.

Stay connected to the latest news, tips, and product updates from Envision. [f](#) [t](#) [in](#) [e](#)

On the presented screen, click **Search** on the left pane without any **Agent Filter Options** selection to search all the latest recordings.

The screenshot shows the Envision Click2Coach Search interface. The left pane contains a 'Search' button highlighted with a red arrow. The main table displays search results for 'John Travel' and 'Beth Bethany'. The table has columns: Agent, Media, Evaluated, Direction, Type, and ID. The first row for 'John Travel' is highlighted with a red border.

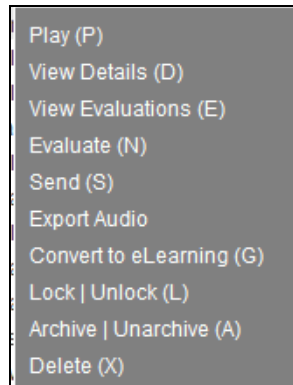
Agent	Media	Evaluated	Direction	Type	ID
John Travel	Audio Only	No	Inbound	FTR	
John Travel	Audio Only	No	Inbound	FTR	
John Travel	Audio Only	No	Inbound	FTR	
Beth Bethany	Audio Only	No	Inbound	FTR	
John Travel	Audio Only	No	Inbound	FTR	
Ronald Reagan	Audio Only	No	Inbound	FTR	
John Travel	Audio Only	No	Inbound	FTR	
Ronald Reagan	Audio Only	No	Inbound	FTR	
Ronald Reagan	Audio Only	No	Inbound	FTR	
Kerry Johnson	Audio Only	No	Inbound	FTR	
Denise Devonshire	Audio Only	No	Inbound	FTR	
Denise Devonshire	Audio Only	No	Inbound	FTR	
Beth Bethany	Audio Only	No	Inbound	FTR	
Denise Devonshire	Audio Only	No	Inbound	FTR	

Double click on the latest recordings and information on the call is shown as below.

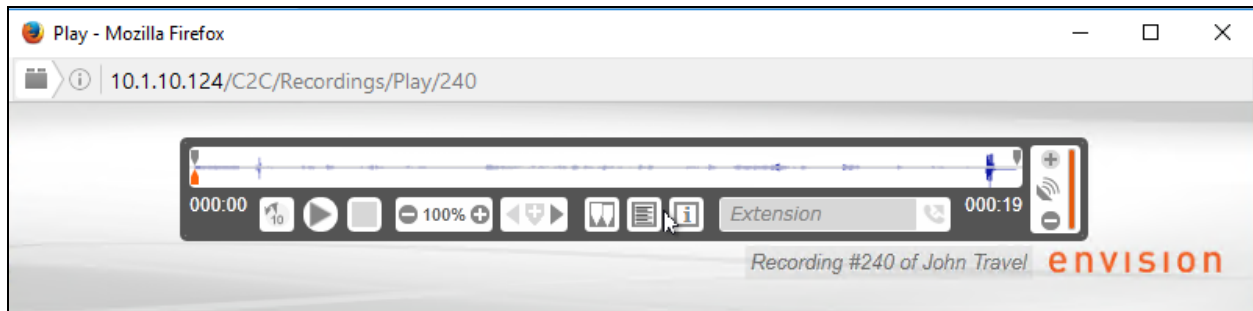
The screenshot shows the Envision Click2Coach Search interface with detailed call information for 'John Travel'. The table has columns: Agent, Media, Evaluated, Direction, Type, and ID. The first row for 'John Travel' is highlighted with a red border.

Agent	Media	Evaluated	Direction	Type	ID
John Travel	Audio Only	No	Inbound	FTR	
Extension : 10001	ANI : 60001	DNIS : 14001	Called Number : N/A	Port : 1	Status : Active
John Travel	Audio Only	No	Inbound	FTR	
John Travel	Audio Only	No	Inbound	FTR	
Beth Bethany	Audio Only	No	Inbound	FTR	
John Travel	Audio Only	No	Inbound	FTR	
Ronald Reagan	Audio Only	No	Inbound	FTR	
John Travel	Audio Only	No	Inbound	FTR	
Ronald Reagan	Audio Only	No	Inbound	FTR	
Ronald Reagan	Audio Only	No	Inbound	FTR	
Kerry Johnson	Audio Only	No	Inbound	FTR	
Denise Devonshire	Audio Only	No	Inbound	FTR	
Denise Devonshire	Audio Only	No	Inbound	FTR	
Beth Bethany	Audio Only	No	Inbound	FTR	

Right click on the **Agent** name to select options like **Play (P)** as shown below.



The following screen pops up. Click on the playback button as below to hear the voice recordings. Verify the whole conversation is recorded.



9. Conclusion

These Application Notes describe the configuration steps required for Envision Click2Coach to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

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

[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 2, Release 7.0.1, May 2016.

[2] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016.

The following Envision product documentation can be obtained from member.

[3] *Envision Click2Coach Installation Guide*, Version 11.5, Jan 2016

[4] *Envision Integrations Guide*, Version 11.5, Dec 2015.

©2016 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.