



Avaya Solution & Interoperability Test Lab

Application Notes for Envision Centricity 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 Centricity to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services for Full Time Recording with Service Observing. Envision Centricity is a call recording solution.

In the compliance testing, Envision Centricity used the Avaya Aura™ Application Enablement Services Device, Media, and Call Control 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.

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 Centricity to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services for Full Time Recording with Service Observing. Envision Centricity is a call recording solution.

In the compliance testing, Envision Centricity 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 Centricity 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.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Envision Centricity:

- Handling of DMCC messages in the areas of call events.
- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC physical device services to activate Service Observing for the virtual IP softphones.
- Use of DMCC monitoring services and media control events to obtain the media from the virtual IP softphones.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous, conference, and transfer.

The serviceability testing focused on verifying the ability of Envision Centricity to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to Envision Centricity.

1.2. Support

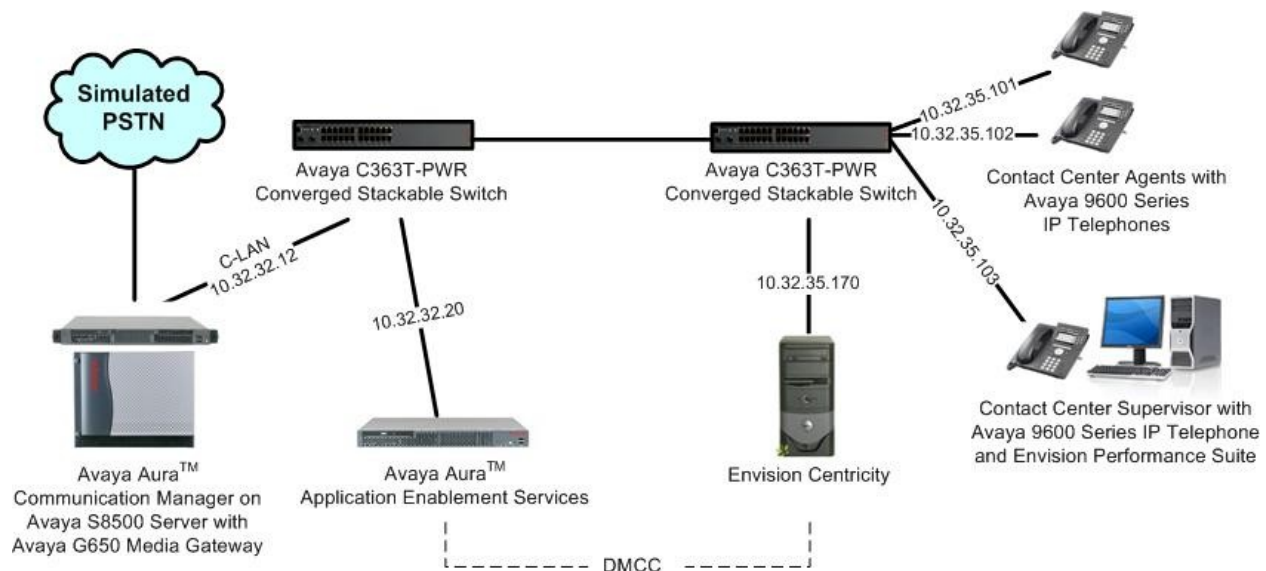
Technical support on Envision Centricity can be obtained through the following:

- **Phone:** (206) 225-0800, x600
- **Email:** support@envisioninc.com
- **Web:** http://www.envisioninc.com/customer_central.cfm

Envision Centricity has a Quality Monitoring application as part of the Performance Suite that can be used to review and playback the call recordings. In the compliance testing, the Envision Performance Suite was installed on the supervisor PC.

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

Device Type	Extension
VDN	65500
Skill Group	65555
Supervisor Station	65000
Agent Station	65001, 65002
Agent ID	65881, 65882



3. Equipment and Software Validated

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

Equipment	Software
Avaya Aura™ Communication Manager on Avaya S8500 Server	R015x.02.1.016.4
Avaya G650 Media Gateway <ul style="list-style-type: none">• TN799DP C-LAN Circuit Pack• TN2302AP IP Media Processor	HW01 FW032 HW20 FW120
Avaya Aura™ Application Enablement Services	5.2
Avaya 9600 Series IP Telephones (H.323)	3.1
Envision Centricity on Windows 2003 Server with Service Pack 2 <ul style="list-style-type: none">• Envision Centricity• Envision Centricity Web Applications• Envision Server• Envision Windows Media Wrapper Service• Avaya DMCC .NET Service Provider	10.0.0202.5 4.2.47.0
Envision Performance Suite	10.0.0100.31

4. Configure Avaya Aura™ Communication Manager

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

- Verify Communication Manager License
- Administer system parameters features
- Administer CTI link
- Administer class of restriction
- Administer agent stations
- Administer virtual IP softphones

4.1. Verify Communication Manager License

Log in to 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 3**. 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 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? n	
Access Security Gateway (ASG)? n	Authorization Codes? n	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? n	CAS Main? n	
Answer Supervision by Call Classifier? n	Change COR by FAC? y	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? n	
ARS/AAR Dialing without FAC? y	DCS (Basic)? n	
ASAI Link Core Capabilities? y	DCS Call Coverage? n	
ASAI Link Plus Capabilities? y	DCS with Rerouting? n	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? n	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n		

4.2. 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 18
                                FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
    Expert Agent Selection (EAS) Enabled? y
    Minimum Agent-LoginID Password Length: 5
    Direct Agent Announcement Extension:          Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
    Converse First Data Delay: 0          Second Data Delay: 2
    Converse Signaling Tone (msec): 100    Pause (msec): 70
    Prompting Timeout (secs): 10

    Reverse Star/Pound Digit For Collect Step? n
    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? n      or Conference Tone? n
    Service Observing Allowed with Exclusion? n
    Allow Two Observers in Same Call? y
```

4.3. Administer CTI Link

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

```
add cti-link 1                                                     Page 1 of 3
                                CTI LINK
  CTI Link: 1
Extension: 60100
  Type: ADJ-IP
                                COR: 1
  Name: Envision CTI Link
```

4.4. 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 2	Page 1 of 23
CLASS OF RESTRICTION	
COR Number: 2	
COR Description:	
FRL: 0	APLT? y
Can Be Service Observed? y	Calling Party Restriction: none
Can Be A Service Observer? y	Called Party Restriction: none
Partitioned Group Number: 1	Forced Entry of Account Codes? n
Priority Queuing? n	Direct Agent Calling? n
Restriction Override: none	Facility Access Trunk Test? n
Restricted Call List? n	Can Change Coverage? n

4.5. 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 4.4**, which allows the station to be service observed.

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

change station 65001	Page 1 of 5	
STATION		
Extension: 65001	Lock Messages? n	BCC: 0
Type: 9630	Security Code: 65001	TN: 1
Port: S00000	Coverage Path 1:	COR: 2
Name: Envision x65001	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 65001	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	Customizable Labels? y	

4.6. 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 “4610”.
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **COR:** The class of restriction number from **Section 4.4**.
- **IP SoftPhone:** “y”

add station 65991		Page 1 of 5
STATION		
Extension: 65991	Lock Messages? n	BCC: 0
Type: 4610	Security Code: 65991	TN: 1
Port: IP	Coverage Path 1:	COR: 2
Name: Envision Virtual #1	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
Speakerphone: 2-way	Personalized Ringing Pattern: 1	
Display Language: english	Message Lamp Ext: 65991	
Survivable GK Node Name:	Mute Button Enabled? y	
Survivable COR: internal	Expansion Module? n	
Survivable Trunk Dest? y	Media Complex Ext:	
	IP SoftPhone? y	
	IP Video Softphone? n	
	Customizable Labels? y	

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 65991
                                     Page 4 of 5

                                     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                        5:
  2: call-appr                        6:
  3: call-appr                        7:
  4: serv-obsrv                     8:

```

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

```

list station 65991 count 2

```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
65991	S00002	Envision Virtual #1				2			
	4610		no			1			
65992	S00005	Envision Virtual #2				2			
	4610		no			1			

5. Configure Avaya Aura™ Application Enablement Services


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

- Verify license
- Launch OAM interface
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI service
- Administer Envision user
- Enable DMCC unencrypted port

5.1. Verify License

Access the Web License Manager interface by using the URL “https://ip-address/WebLM/index.jsp” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Web License Manager** screen is displayed. Log in using the appropriate credentials.



The **Web License Manager** screen is displayed. 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.

AVAYA Web License Manager (WebLM v4.6) Logoff

Install License

Licensed Products

▼ **APPL_ENAB**

Application_Enablement

Uninstall License

Change Password

Server Properties

Manage Users

Logout

Application Enablement (CTI) - Release: 5 - SID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: Apr 16, 2010 11:27:38 AM EDT

[View Peak Usage](#)

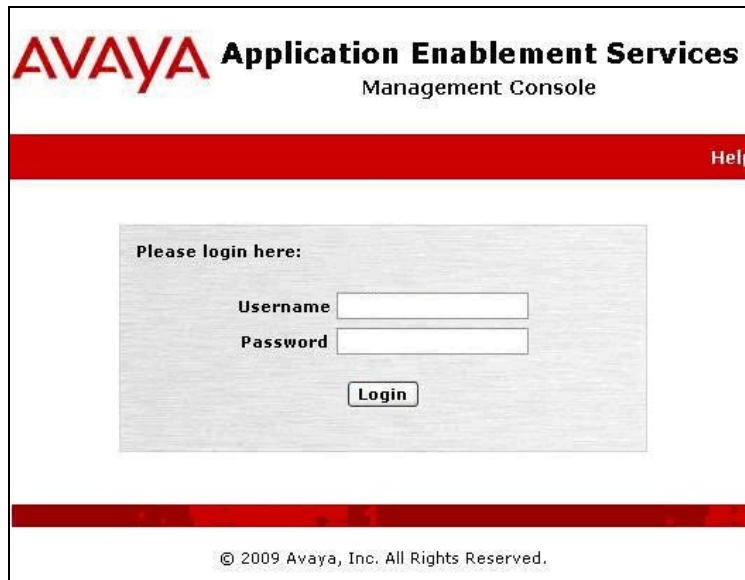
Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	100	0
DLG (VALUE_AES_DLG)	permanent	16	0
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	0

5.2. Launch OAM Interface

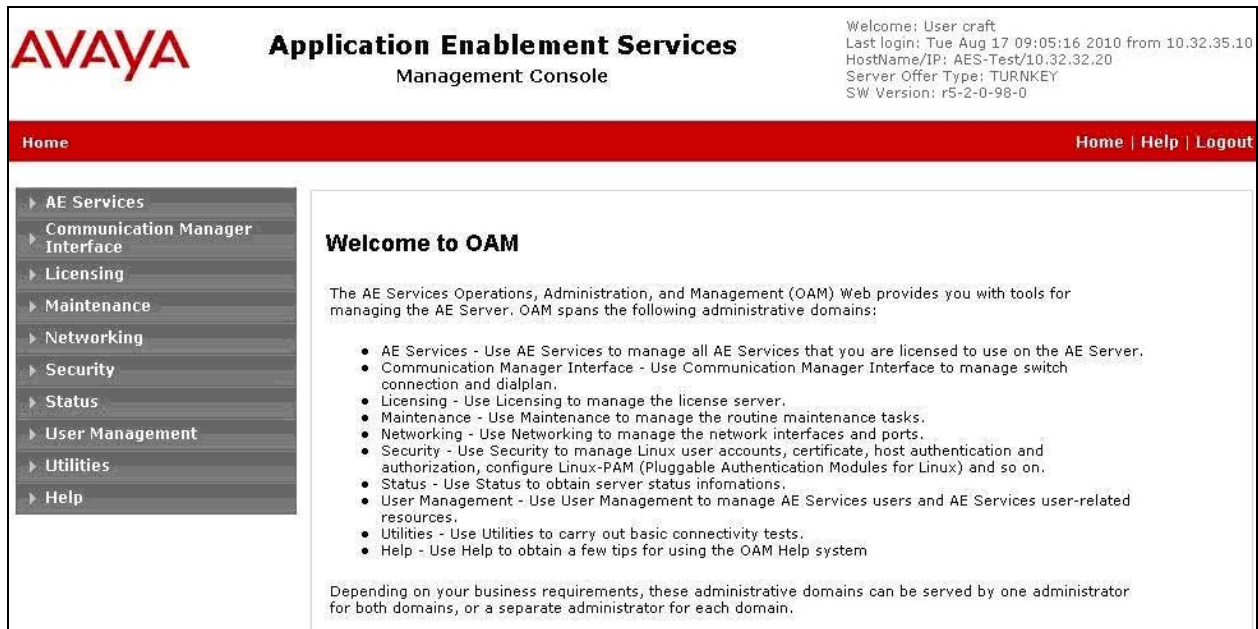
Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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



The screenshot shows the login page of the AVAYA Application Enablement Services Management Console. At the top, the AVAYA logo is on the left, and the text "Application Enablement Services Management Console" is on the right. Below this is a red horizontal bar with the word "Help" in white on the right side. The main content area is a light gray box with the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a "Login" button. At the bottom of the page, there is a red horizontal bar and the copyright notice "© 2009 Avaya, Inc. All Rights Reserved."

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



The screenshot shows the "Welcome to OAM" screen of the AVAYA Application Enablement Services Management Console. At the top, the AVAYA logo is on the left, and the text "Application Enablement Services Management Console" is on the right. To the right of the header, there is a welcome message: "Welcome: User craft", "Last login: Tue Aug 17 09:05:16 2010 from 10.32.35.10", "HostName/IP: AES-Test/10.32.32.20", "Server Offer Type: TURNKEY", and "SW Version: r5-2-0-98-0". Below the header is a red horizontal bar with the word "Home" on the left and "Home | Help | Logout" on the right. The main content area is divided into two sections. On the left is a sidebar with a list of links: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". On the right is the "Welcome to OAM" section, which contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their functions. At the bottom of the main content area, there is a paragraph: "Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain."

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Tue Aug 17 09:05:16 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Home | Help | Logout

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

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

5.3. 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 "craft" with login details. A red navigation bar contains "AE Services | TSAPI | TSAPI Link" and links for "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links", and "TSAPI Properties". The main content area is titled "TSAPI Links" and features a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are three buttons: "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8500" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 4.3**. Retain the default values in the remaining fields, and click **Apply Changes**.

The screenshot shows the "Add TSAPI Links" screen in the AVAYA Application Enablement Services Management Console. The layout is similar to the previous screen, but the main content area contains a form with the following fields: "Link" (value: 1), "Switch Connection" (value: S8500), "Switch CTI Link Number" (value: 1), "ASAI Link Version" (value: 4), and "Security" (value: Unencrypted). At the bottom of the form are two buttons: "Apply Changes" and "Cancel Changes".

5.4. 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 “S8500”, 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 is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. There is one entry with Connection Name 'S8500', Processor Ethernet 'No', Msg Period '30', and Number of Active Connections '0'. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', and 'Delete Connection'. The 'Edit H.323 Gatekeeper' button is highlighted.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8500	No	30	0

The **Edit H.323 Gatekeeper** 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 “10.32.32.12” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8500' screen. The left navigation pane is the same as the previous screenshot. The main content area has a title 'Edit H.323 Gatekeeper - S8500'. Below the title is a text input field containing '10.32.32.12' and a button 'Add Name or IP'. Below the input field is a label 'Name or IP Address' and a button 'Delete IP'.

5.5. Disable Security Database

Select **Security > Security Database > Control** from the left pane, to display the **SDB Control for DMCC and TSAPI** screen in the right pane. Uncheck **Enable SDB TSAPI Service, JTAPI and Telephony Service**, 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 and TSAPI' and contains two checkboxes: 'Enable SDB for DMCC Service' (checked) and 'Enable SDB TSAPI Service, JTAPI and Telephony Service' (unchecked). An 'Apply Changes' button is at the bottom.

Welcome: User craft
Last login: Tue Aug 17 09:05:16 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Security | Security Database | Control

Home | Help | Logout

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control

SDB Control for DMCC and TSAPI

☒ Enable SDB for DMCC Service
☐ Enable SDB TSAPI Service, JTAPI and Telephony Service
Apply Changes

5.6. Restart TSAPI Service

Select **Maintenance > Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **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' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked. Below the table is a note: 'For status on actual services, please use Status and Control'. At the bottom are buttons for 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'.

Welcome: User craft
Last login: Tue Aug 17 09:05:16 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Maintenance | Service Controller

Home | Help | Logout

AE Services
Communication Manager Interface
Licensing
Maintenance
Date Time/NTP Server
Security Database
Service Controller
Server Data
Networking
Security
Status
User Management

Service Controller

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

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

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

5.7. 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).

AVAYA

Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Aug 17 09:05:16 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id	<input type="text" value="envision"/>
* Common Name	<input type="text" value="envision"/>
* Surname	<input type="text" value="envision"/>
* User Password	<input type="password" value="....."/>
* Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>

5.8. Enable DMCC Unencrypted Port

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

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

AVAYA

Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Aug 17 09:05:16 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

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

DLG Port

TCP Port	5678			
----------	------	--	--	--

TSAPI Ports

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

DMCC Server Ports

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

6. Configure Envision Centricity

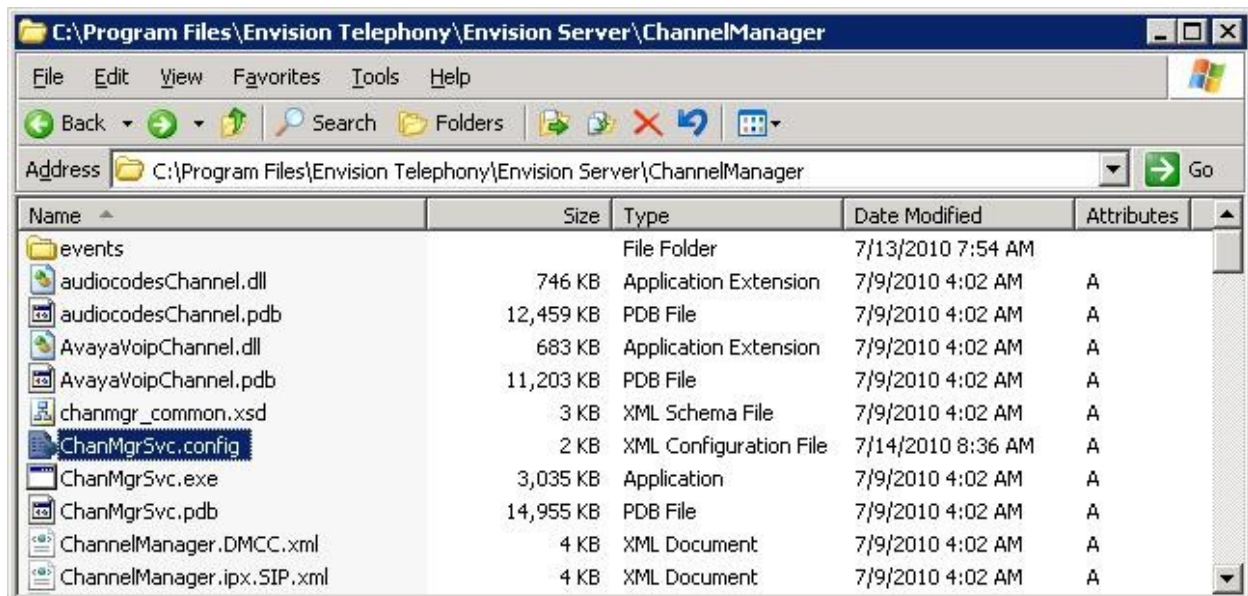
This section provides the procedures for configuring Envision Centricity. The procedures include the following areas:

- Administer ChanMgrSvc.config
- Administer ChannelManager.xml
- Launch Administrator
- Administer system settings
- Administer telephony settings
- Administer telephony Envision servers
- Administer telephony device IDs
- Administer users
- Restart services
- Administer channels

The configuration of Centricity 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.

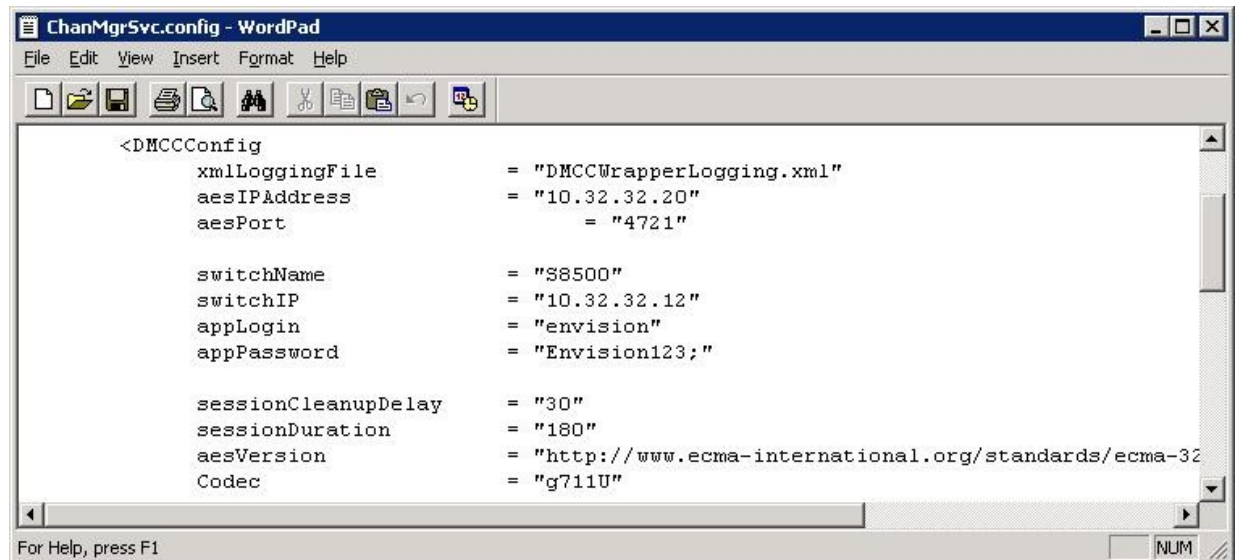
6.1. Administer ChanMgrSvc.config

From the Centricity server, navigate to the **C:\Program Files\Envision Telephony\Envision Server\ChannelManager** directory to locate the **ChanMgrSvc.config** file shown below.



Open the **ChanMgrSvc.config** file with the Windows WordPad application. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **aesIPAddress:** IP address of the Application Enablement Services server.
- **switchName:** Switch connection name from **Section 5.3**.
- **switchIP:** IP address of the H.323 gatekeeper from **Section 5.4**.
- **appLogin:** Envision user credentials from **Section 5.7**.
- **appPassword:** Envision user credentials from **Section 5.7**.



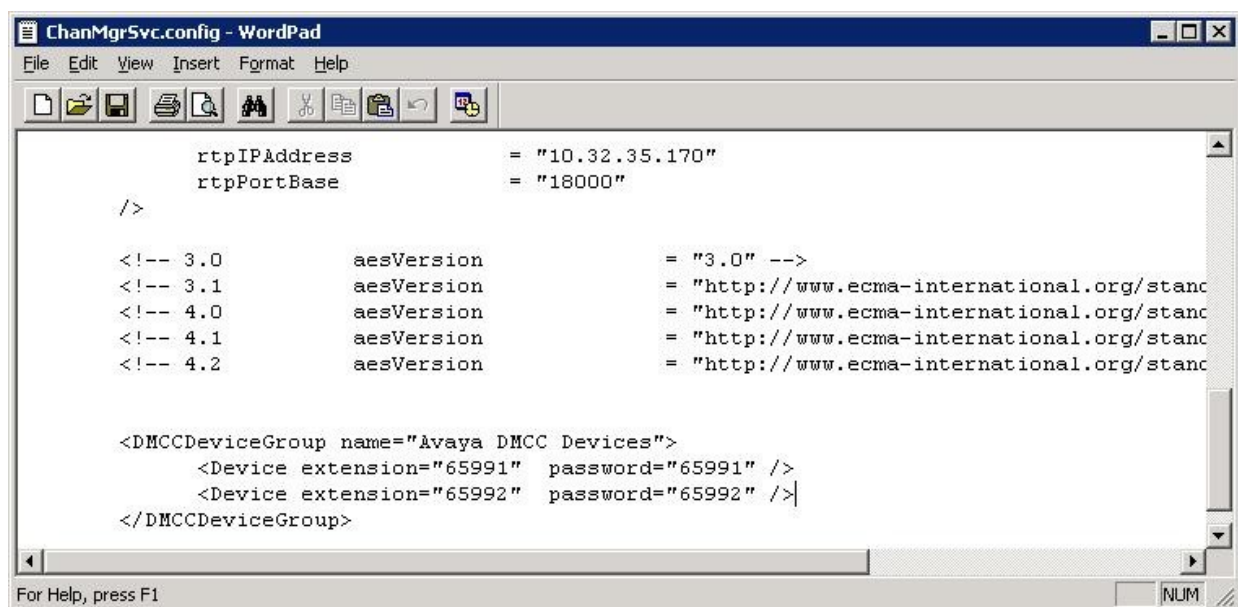
```

<DMCCConfig
  xmlLoggingFile      = "DMCCWrapperLogging.xml"
  aesIPAddress        = "10.32.32.20"
  aesPort             = "4721"

  switchName          = "S8500"
  switchIP            = "10.32.32.12"
  appLogin            = "envision"
  appPassword         = "Envision123;"

  sessionCleanupDelay = "30"
  sessionDuration     = "180"
  aesVersion          = "http://www.ecma-international.org/standards/ecma-32
  Codec               = "g711U"
  
```

Scroll to the bottom of the screen. For **rtpIPAddress**, enter the IP address of the Envision server. In the **DMCCDeviceGroup** section, create an entry line with the extension and password for each virtual IP softphone from **Section 4.6**, as shown below.



```

  rtpIPAddress        = "10.32.35.170"
  rtpPortBase         = "18000"
/>

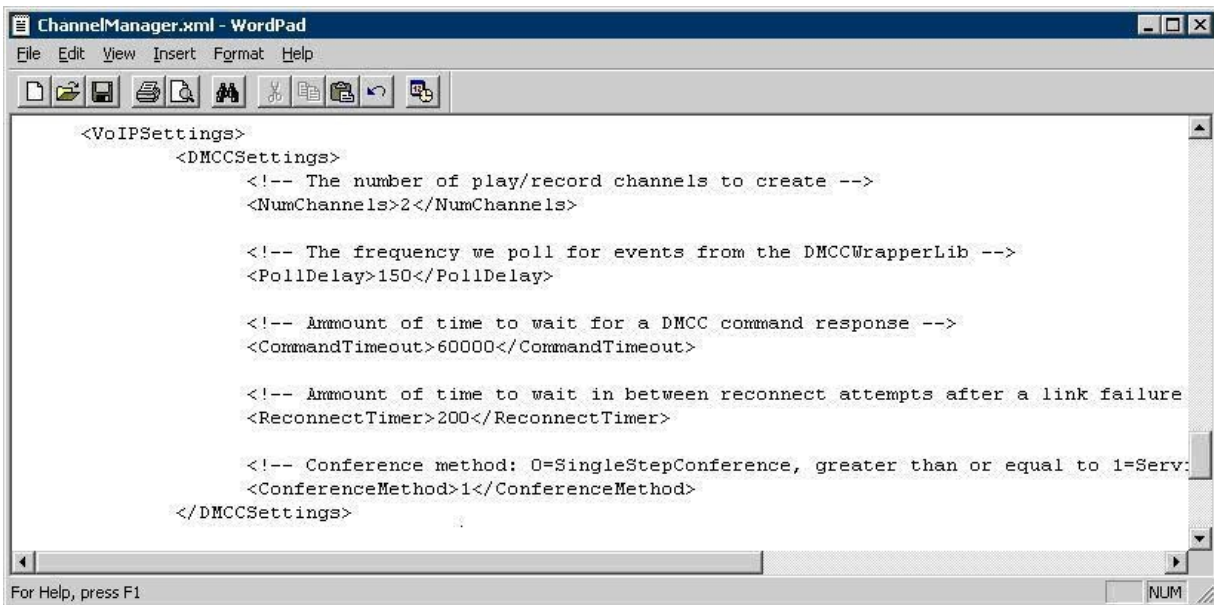
<!-- 3.0      aesVersion          = "3.0" -->
<!-- 3.1      aesVersion          = "http://www.ecma-international.org/stanc
<!-- 4.0      aesVersion          = "http://www.ecma-international.org/stanc
<!-- 4.1      aesVersion          = "http://www.ecma-international.org/stanc
<!-- 4.2      aesVersion          = "http://www.ecma-international.org/stanc

<DMCCDeviceGroup name="Avaya DMCC Devices">
  <Device extension="65991" password="65991" />
  <Device extension="65992" password="65992" />
</DMCCDeviceGroup>
  
```

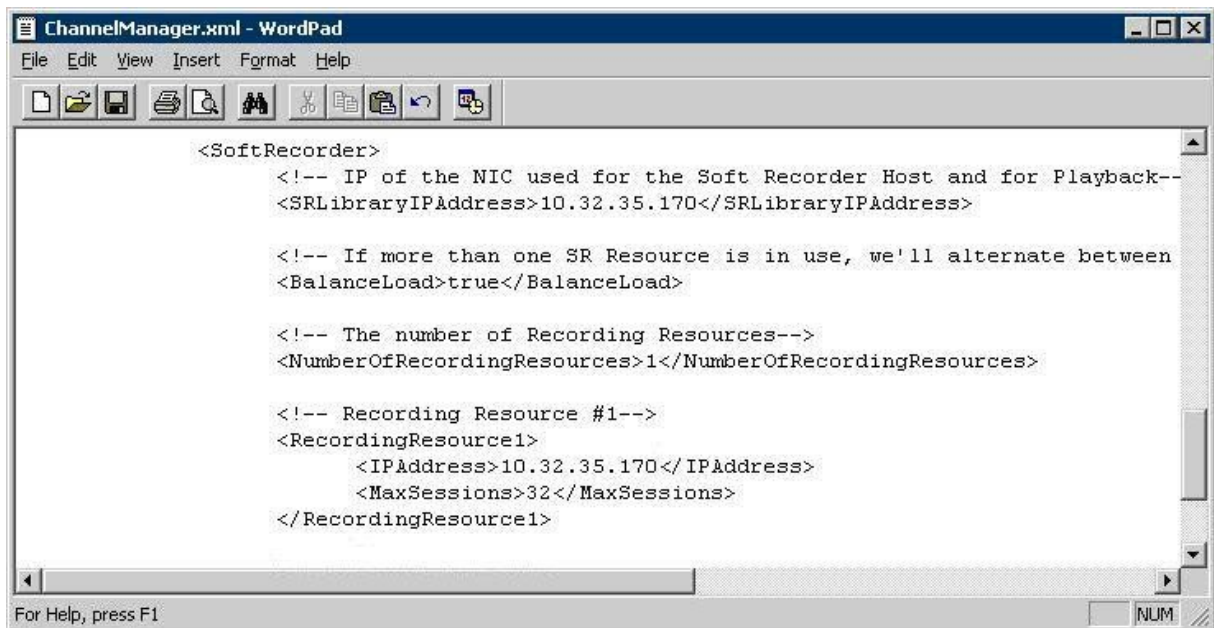
6.2. Administer ChannelManager.xml

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

Scroll down to the **DMCCSettings** section. For **ReconnectTimer**, enter “200”. For **ConferenceMethod**, enter “1” to enable Service Observing.

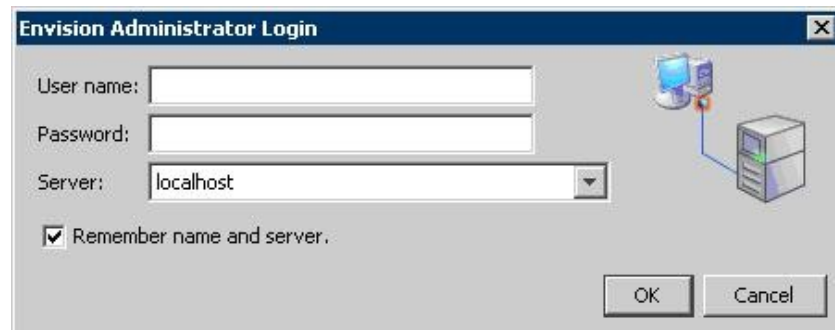


Scroll down to the **SoftRecorder** section. For **SRLibraryIPAddress** and **RecordingResource1 IPAddress**, enter the IP address of the Envision server as shown below.

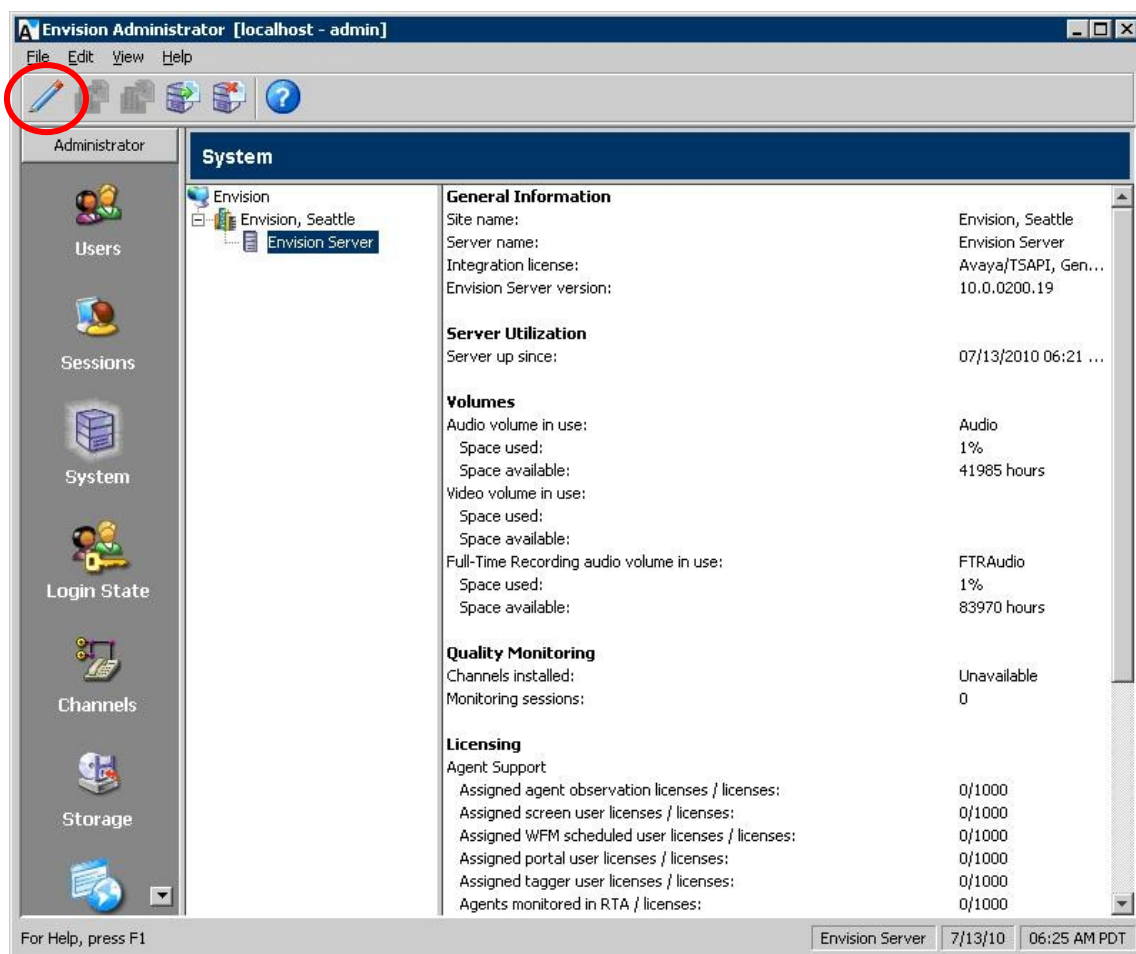


6.3. Launch Administrator

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

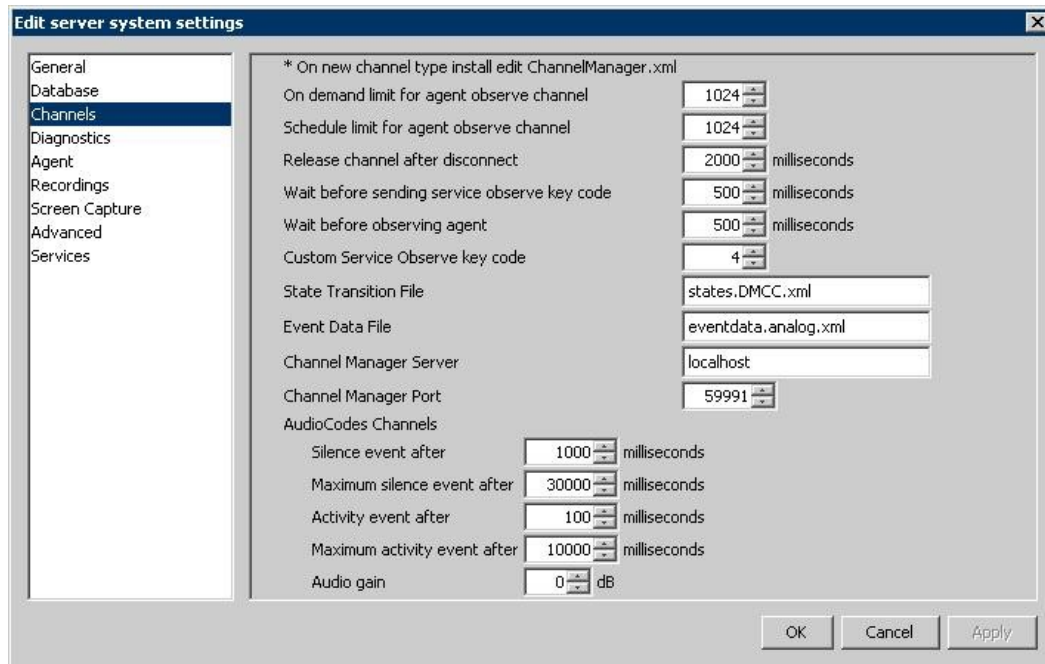


The **Envision Administrator** screen is displayed, and the right pane defaults to the **System** screen. Click on the **Edit system settings** icon.

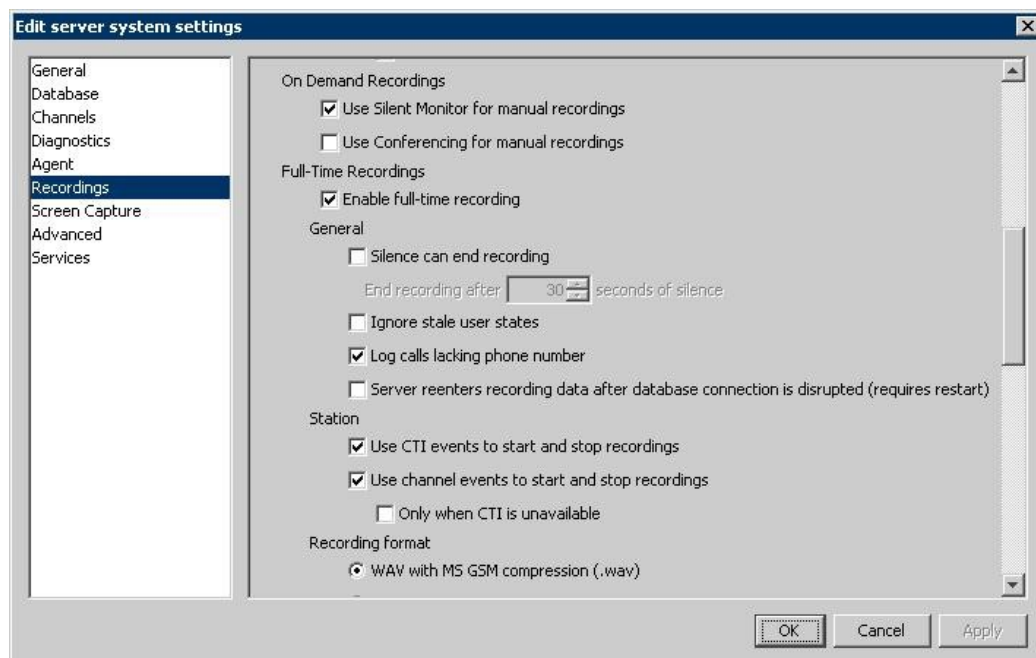


6.4. Administer System Settings

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 4.6**.



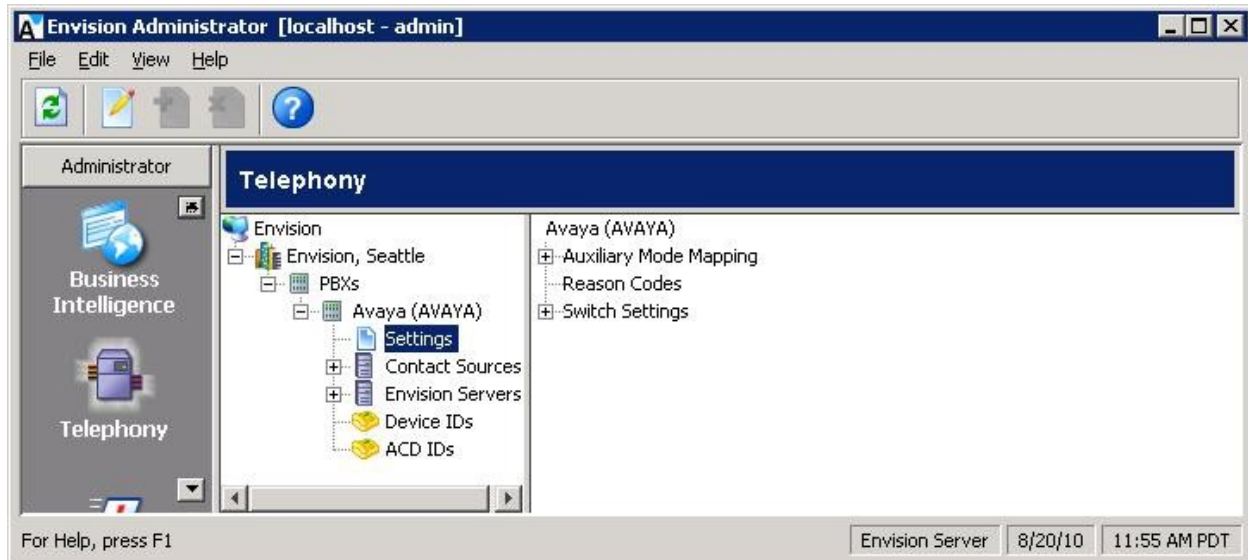
Select **Recordings** from the left pane, and scroll the screen down to the **Full-Time Recordings** section. Check **Enable full-time recording**, as shown below.



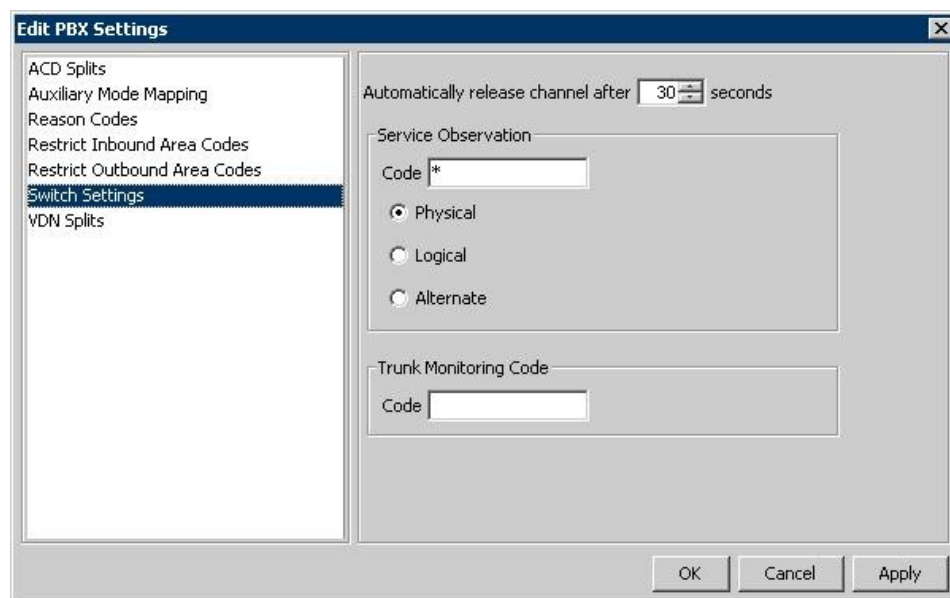
6.5. Administer Telephony Settings

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

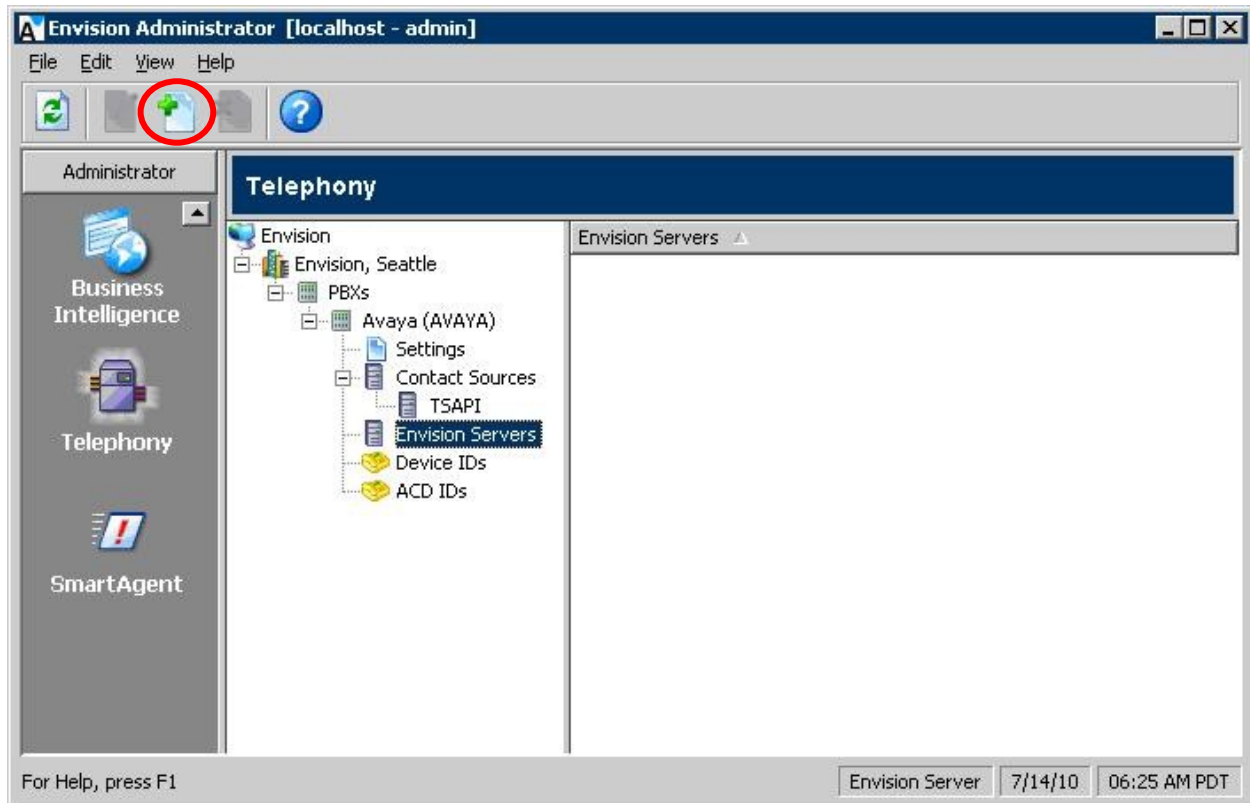


The **Edit PBX Settings** screen is displayed. Select **Switch Settings** from the left pane. For **Service Observation Code**, enter a non-blank value to denote this method being used. Retain the default values in the remaining fields.



6.6. Administer Telephony Envision Servers

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

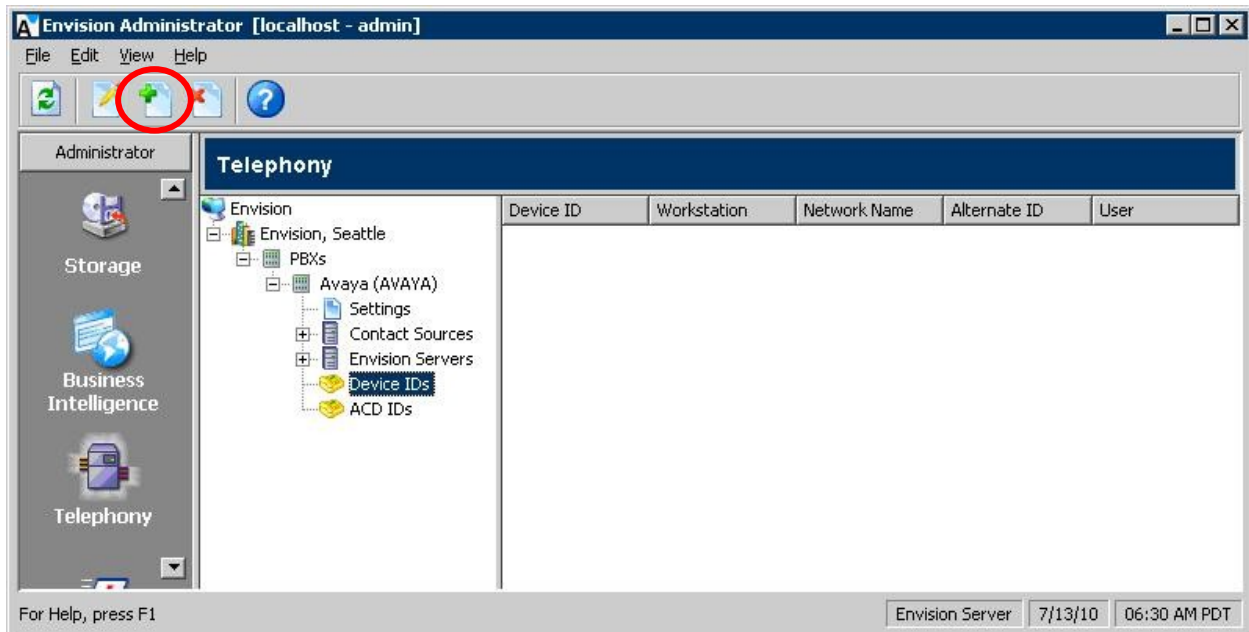


The **Assign Envision Server** screen is displayed. Select the proper **Envision Server**, as shown below.



6.7. Administer Telephony Device IDs

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



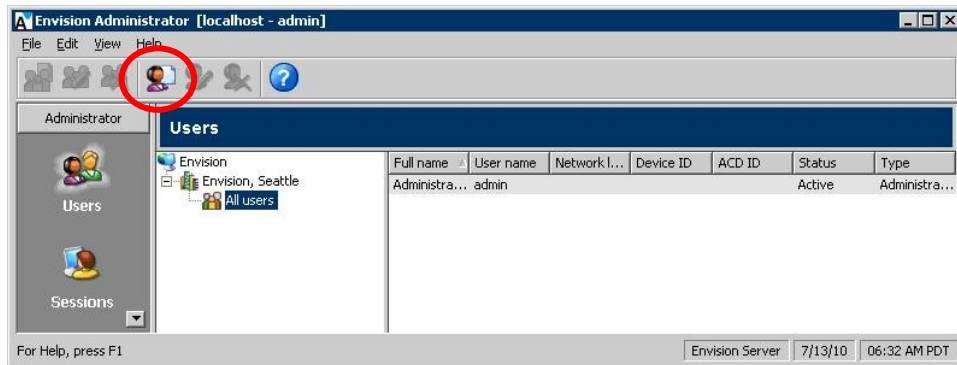
The **Add Device IDs** screen is displayed. Create a device ID for each agent station from **Section 2**. Note that ranges can be used for consecutive agent stations, as shown below.

The screenshot shows the "Add Device IDs" dialog box. It has a title bar with the text "Add Device IDs" and a close button. The dialog contains the following fields and controls:

- "First Device ID" text box with the value "65001" and a spinner control.
- "Last Device ID" text box with the value "65002" and a spinner control.
- "Workstation" text box.
- "Network Name" text box.
- An unchecked checkbox labeled "Alternate ID".
- A text box below the checkbox containing the value "1" and a spinner control.
- "OK" and "Cancel" buttons at the bottom right.

6.8. 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.

The 'Create New User Account' dialog box has tabs for 'General', 'Privileges', 'Assignments', 'Agent components', 'View', and 'Certificates'. The 'General' tab is active.

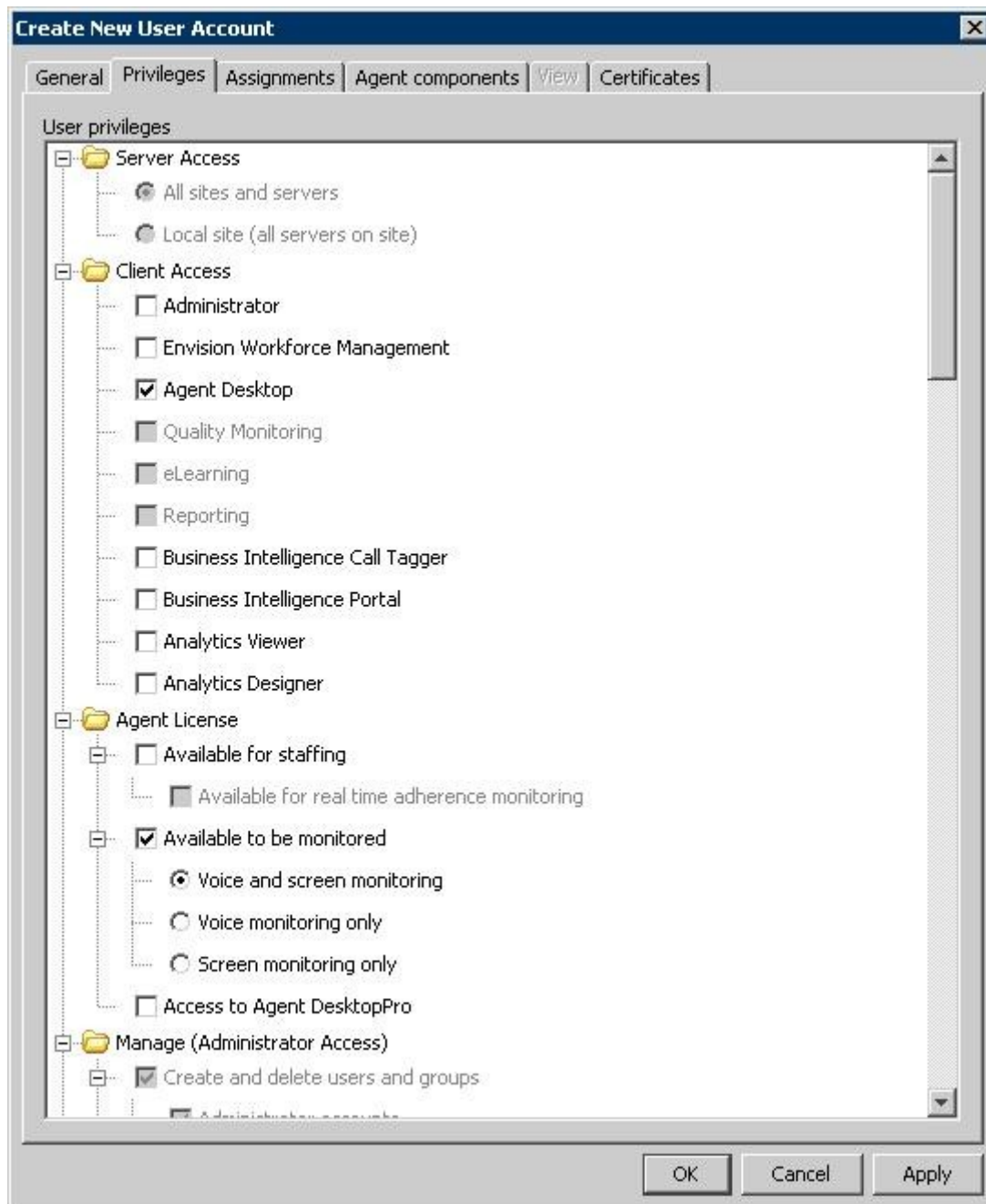
Fields and controls include:

- Domain name: [text box]
- Network login name: [text box]
- User name *: [text box with 'Agent65001']
- Full name *: [text box with 'Agent65001']
- Change password...: [button]
- * Required Field: [text]
- PBX: [dropdown menu with 'Avaya']
- Device ID: [dropdown menu with '65001']
- ACD ID: [empty text box]
- Account: [group box containing:
 - ☐ Inactive
 - ☒ Active
 - ☐ Active until: [date picker set to 07/13/2010]

A calendar widget shows the month of July 2010.

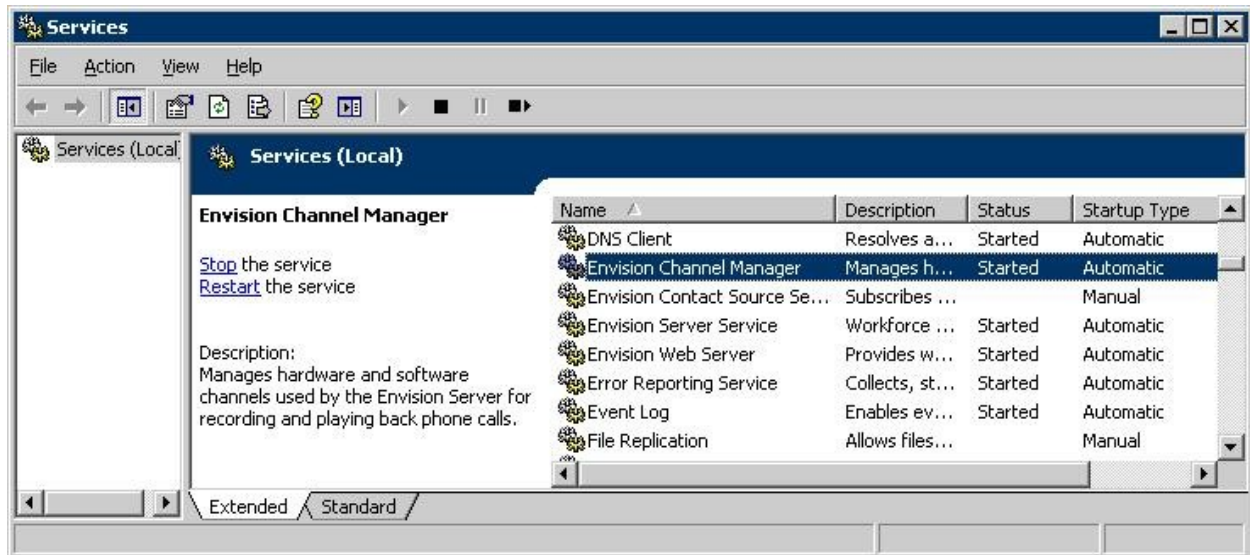
Buttons at the bottom: OK, Cancel, Apply.

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.



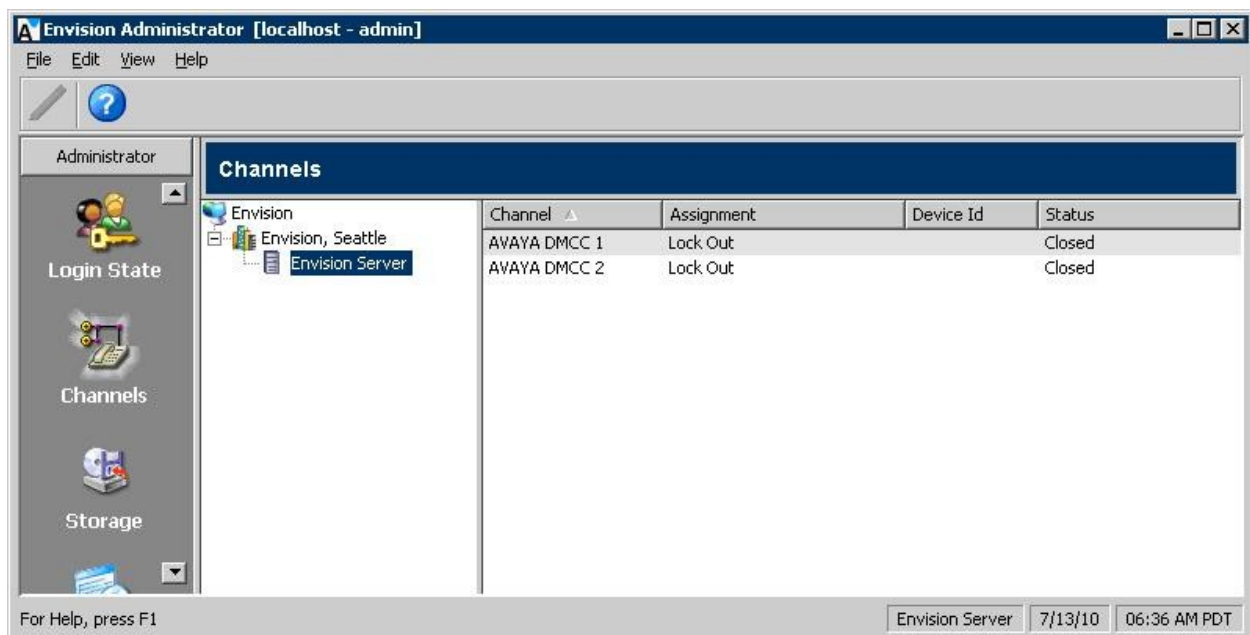
6.9. Restart Services

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.

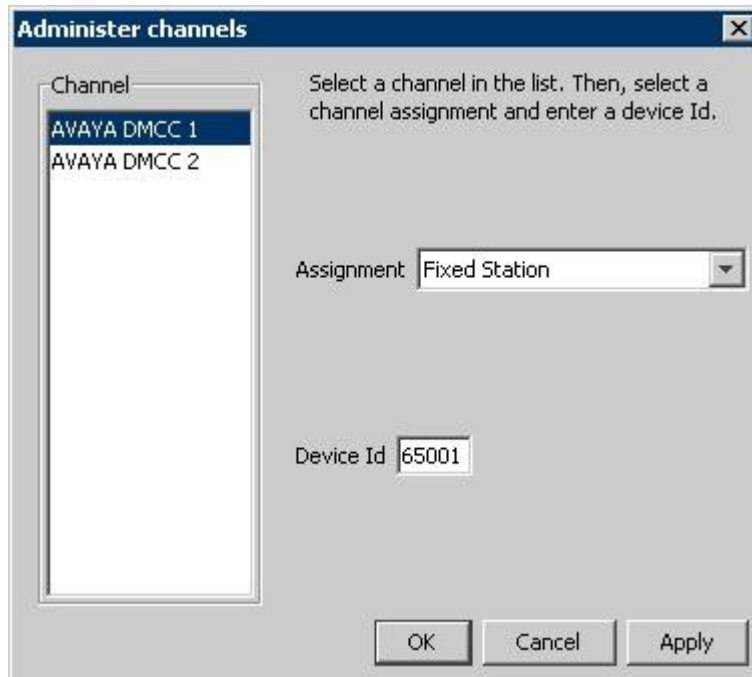


6.10. Administer Channels

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 channels.



The image shows a Windows-style dialog box titled "Administer channels". On the left, there is a list box labeled "Channel" containing two items: "AVAYA DMCC 1" (which is highlighted) and "AVAYA DMCC 2". 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 dropdown menu labeled "Assignment" with "Fixed Station" selected. Further down, there is a text input field labeled "Device Id" containing the value "65001". At the bottom right of the dialog box, there are three buttons: "OK", "Cancel", and "Apply".

7. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Envision Centricity application, the application uses Avaya AuraTM Application Enablement Services DMCC to automatically register the virtual IP softphones to Avaya AuraTM 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.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to Envision Centricity.

The verification of tests included using the Envision Centricity logs for proper message exchanges, and using the Envision Quality Monitoring application for proper logging and playback of the calls.

All test cases were executed and passed. The following were the observations on Envision Centricity from the compliance testing.

- In the transfer/conference scenarios, the recording associated with the transfer-from/conference-from agents contain silence for the period from the initiation to the completion of the transfer/conference.
- 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.
- Removing a previously monitored agent station on Avaya AuraTM Communication Manager can lead to a link re-establishment by the application.

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 Centricity.

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 4.3**, 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
1	4	no	AES-Test	established	26	19

Verify the registration status of the virtual softphones by using the “list registered-ip-stations” command. Verify that the virtual IP softphones from **Section 4.6** are displayed, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address		
65000	9640	IP_Phone	y	10.32.35.105		
	1	3.10000		10.32.32.12		
65001	9630	IP_Phone	y	10.32.35.101		
	1	3.10000		10.32.32.12		
65002	9630	IP_Phone	y	10.32.35.106		
	1	3.1000		10.32.32.12		
65991	4610	IP_API_A	y	10.32.32.20		
	1	3.2040		10.32.32.12		
65992	4610	IP_API_A	y	10.32.32.20		
	1	3.2040		10.32.32.12		

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. In the lower portion of the screen, verify that the **User** column shows an active session with the Envision user name from **Section 5.7**, and that the **# of Associated Devices** column reflects the number of station extensions from **Section 2** plus the number of virtual softphones from **Section 4.6**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User: craft
Last login: Tue Apr 20 11:15:31 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Status | Status and Control | DMCC Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ **DMCC Service Summary**

■ Switch Conn Summary

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Tue Apr 20 11:50:01 EDT 2010

Service Uptime: 0 days, 0 hours 56 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 5

Number of Existing Devices: 4

Number of Devices Created Since Service Boot: 20

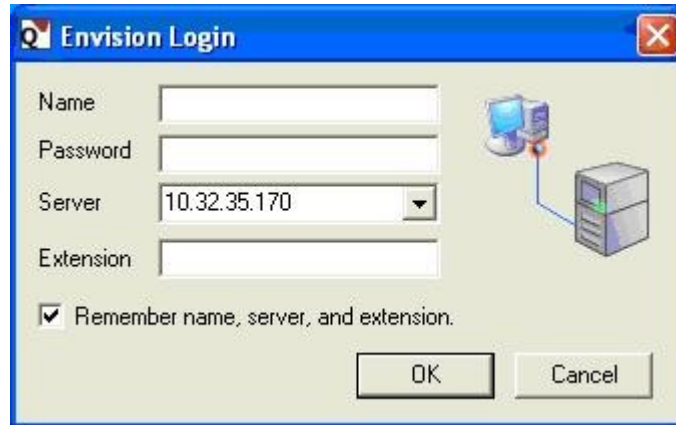
Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/> 95F8C143240F724074CFD63171837873-4	envision	S8500	10.32.35.175	XML Unencrypted	4

Terminate Sessions Show Terminated Sessions

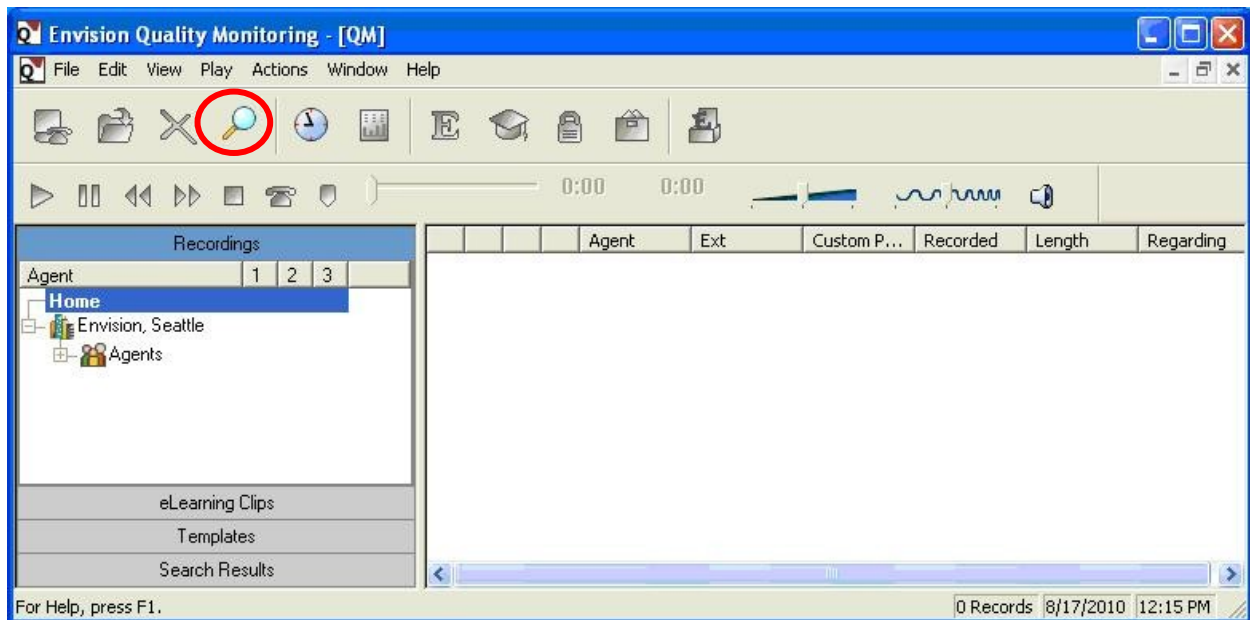
8.3. Verify Envision Centricity

Log an agent in to the Skill group to handle and complete an ACD call. From the supervisor PC, select **Start > Programs > Envision Telephony > Envision Performance Suite > Quality Monitoring** to launch the **Quality Monitoring** application.

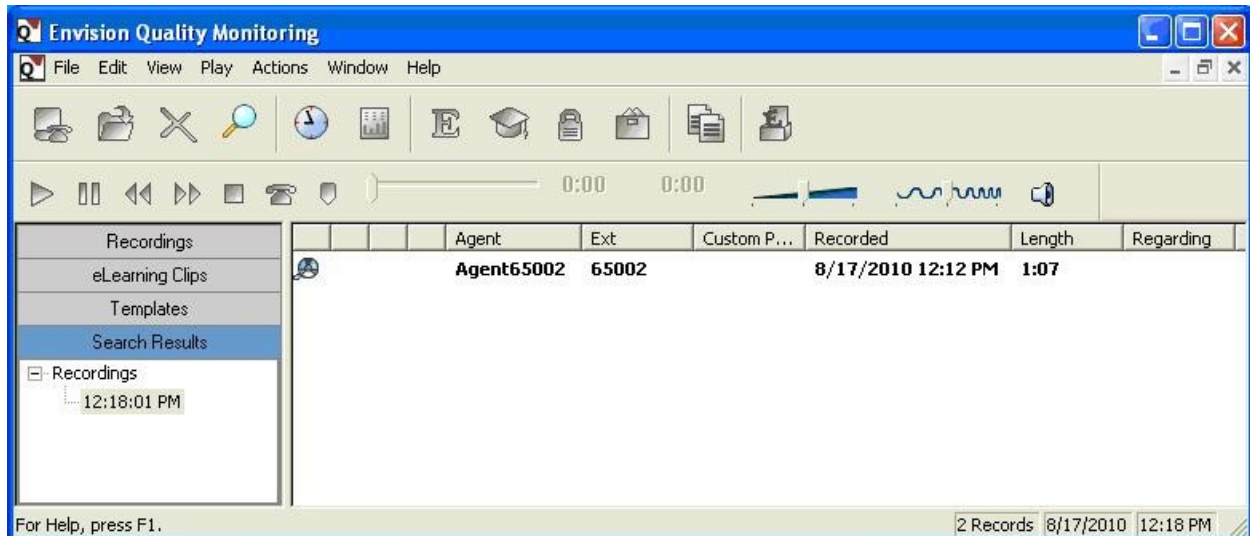
The **Envision Login** screen is displayed. For **Server**, select the IP address of the Centricity server. Enter the appropriate credentials.



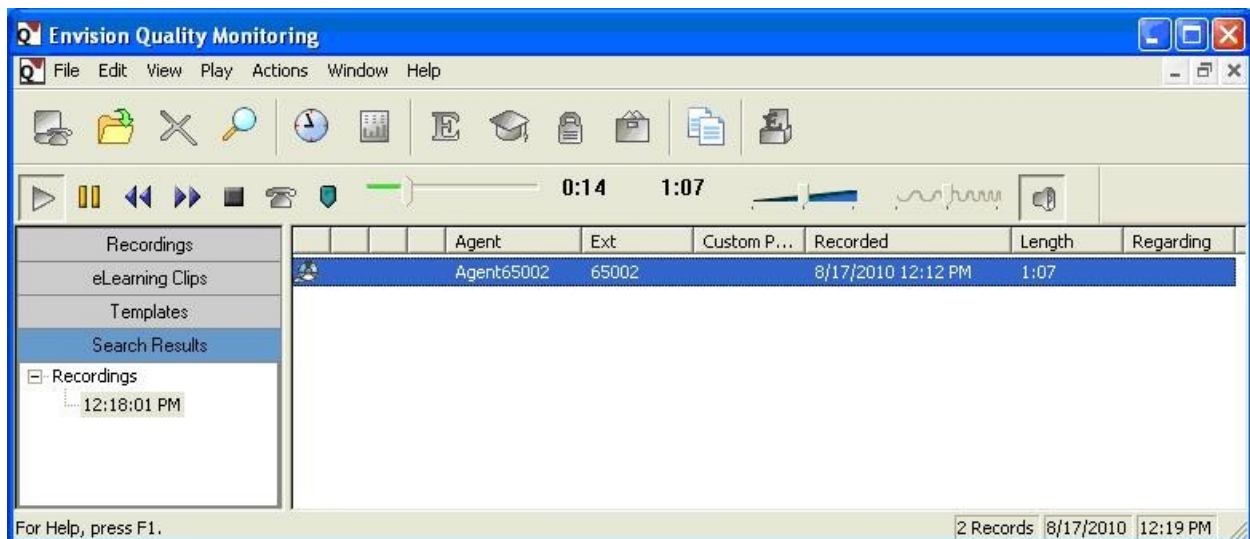
The **Envision Quality Monitoring** screen is displayed. Click on the **Search** icon shown below. The **Search for Recordings** screen is displayed next (not shown below), retain all default values to enable search for all recordings for the current day.



The **Envision Quality Monitoring** screen is updated with the search result. Verify that there is an entry reflecting the call, with proper values in the relevant fields. Double click on the entry to listen to the playback.



Verify that the call recording is played back.



9. Conclusion

These Application Notes describe the configuration steps required for Envision Centricity 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 7**.

10. Additional References

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

1. *Administrator Guide for Avaya Aura™ Communication Manager*, Document 03-300509, Issue 5.0, Release 5.2, May 2009, available at <http://support.avaya.com>.
2. *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, Release 5.2, Document ID 02-300357, Issue 11, November 2009, available at <http://support.avaya.com>.
3. *Envision Administrator Guide*, Version 10, available on the Envision server as part of installation.
4. *Envision Quality Monitoring User's Guide*, Version 10, available as part of the Envision Performance Suite installation.

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.