



Avaya Solution & Interoperability Test Lab

Application Notes for Envision Centricity with Avaya Proactive Contact with PG230 and Avaya Aura® Application Enablement Services for Quality Monitoring with Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Envision Centricity to interoperate with Avaya Proactive Contact with PG230 and Avaya Aura® Application Enablement Services for Quality Monitoring with Service Observing. Envision Centricity is a call recording solution.

In the compliance testing, Envision Centricity used the Event Services interface from Avaya Proactive Contact to obtain information on agent states and call status, and used the Service Observing feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture the 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 Proactive Contact with PG230 and Avaya Aura® Application Enablement Services for Quality Monitoring with Service Observing. Envision Centricity is a call recording solution.

In the compliance testing, Envision Centricity used the Event Services interface from Avaya Proactive Contact to obtain information on agent states and call status, and used the Service Observing feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture the media associated with the monitored agents for call recording.

In a Quality Monitoring environment, recording of calls at the agents are controlled by the agent recording schedule defined by the supervisor using the Envision Quality Monitoring application. For agents with active schedules, Envision Centricity uses the Event Services interface to monitor calls at the agents, and to obtain the media associated with the calls for recording. The media is obtained by using DMCC to activate the Service Observing feature to enable a virtual IP softphone to observe and to join the call at the agent.

This compliance test covered the recording of calls using the Avaya Proactive Contact with PG230 deployment option and call blending. The results should be applicable to the Avaya Proactive Contact Standalone deployment option with call blending.

2. 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 automatically checks the state of the virtual IP softphones using DMCC and obtains system statistics using Event Services.

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 Avaya Proactive Contact Agent application to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection 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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

- 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.
- Handling of real-time agent states and call events from Avaya Proactive Contact.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, agent drop, customer drop, hold, reconnect, simultaneous agent recordings, conference, transfer, supervised/unsupervised forward work, and call blending scenarios.

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

2.2. Test Results

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

- The Service Observing confirmation tone overlays the first ~3 seconds of the recordings due to system in process of assigning recording channel. Dedicated channels can be set up as an alternative to avoid confirmation tones in the recordings.
- If the seized virtual IP softphone fails the registration due to invalid credentials, then the call will not be recorded. This is addressed as part of system implementation when Envision Professional Services validate all configured virtual IP softphones can register and record properly.
- In a failed Service Observing scenario, the recording contains the denial tone followed by silence.
- In the rare event that the virtual IP softphone became unregistered at Communication Manager, Centricity will receive an error when requests the un-registration and cannot record subsequent calls. The workaround is to manually restart the Centricity application.
- In the supervised forward with transfer/conference scenarios, the recording for both agents will stop after the transfer-from/conference-from agent drops from the call.

2.3. 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

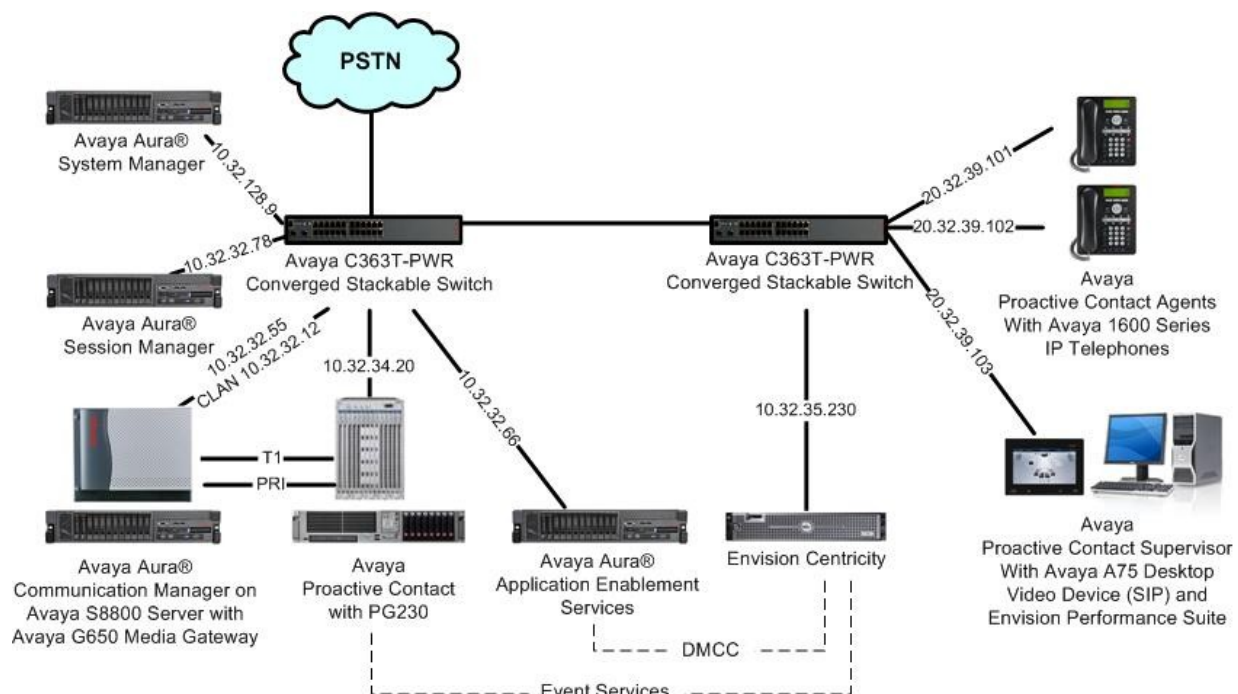
3. Reference Configuration

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.

The configuration of Avaya Aura® Session Manager is performed via the web interface of Avaya Aura® System Manager. The detailed administration of basic connectivity between Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described. Furthermore, the detailed administration of agent recording schedules on Envision Quality Monitoring is outside the scope of these Application Notes and will not be described.

In the compliance testing, Envision Centricity monitored the Proactive Contact agents shown in the table below.

Device Type	Value
Agent Station Extension	65001, 65002
Agent Headset Number	105, 106



4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP2 (R016x.00.1.510.1-18860)
Avaya G650 Media Gateway <ul style="list-style-type: none">TN799DP C-LAN Circuit PackTN2302AP IP Media Processor	HW01 FW038 HW20 FW122
Avaya Proactive Contact with PG230	4.2
Avaya Aura® Application Enablement Services	6.1
Avaya Aura® Session Manager	6.1 SP2
Avaya Aura® System Manager	6.1 SP2
Avaya 1600 Series IP Telephones (H.323)	1.3
Avaya A175 Desktop Video Device (SIP)	1.0.2
Envision Centricity on Windows 2008 Server with Service Pack 2 <ul style="list-style-type: none">Envision CentricityEnvision Centricity Web ApplicationsEnvision ServerEnvision Windows Media Wrapper ServiceAvaya DMCC .NET Service Provider	10.1.0000.394 4.2.47.0
Envision Performance Suite	10.1.0000.394

5. Configure Avaya Aura® Communication Manager

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

- Administer system parameters features
- Administer class of restriction
- Administer agent stations
- Administer virtual IP softphones

5.1. 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: 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
    Interflow-qpos EWT Threshold: 2
    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
```

5.2. 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: 7		APLT? y	
Can Be Service Observed? y		Calling Party Restriction: outward	
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? n	
Restriction Override: none		Facility Access Trunk Test? n	
Restricted Call List? n		Can Change Coverage? n	

5.3. Administer Agent Stations

Modify each physical station used by the Proactive Contact 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 5.2**, which allows the station to be service observed.

Repeat this section for all agent stations in **Section 3**.

change station 65001		Page 1 of 5	
STATION			
Extension: 65001	Lock Messages? n	BCC: 0	
Type: 1616	Security Code: 65001	TN: 1	
Port: S00000	Coverage Path 1: 1	COR: 2	
Name: Avaya H323 #1	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
	Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1		
	Message Lamp Ext: 65001		
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? n		
	IP Video? n		
	Short/Prefixed Registration Allowed: default		

5.4. 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 “4620”.
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **COR:** The class of restriction number from **Section 5.2**.
- **IP SoftPhone:** “y”

add station 65991		Page 1 of 5
STATION		
Extension: 65991	Lock Messages? n	BCC: 0
Type: 4620	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:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 65991	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Expansion Module? n	
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	

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 IP softphones.

add station 65991Page 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 3**.

list station 65991 count 2

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack		
65991	S00020	Envision Virtual #1				2			
	4620		no			1	1		
65992	S00039	Envision Virtual #2				2			
	4620		no			1	1		

6. Configure Avaya Aura® Application Enablement Services

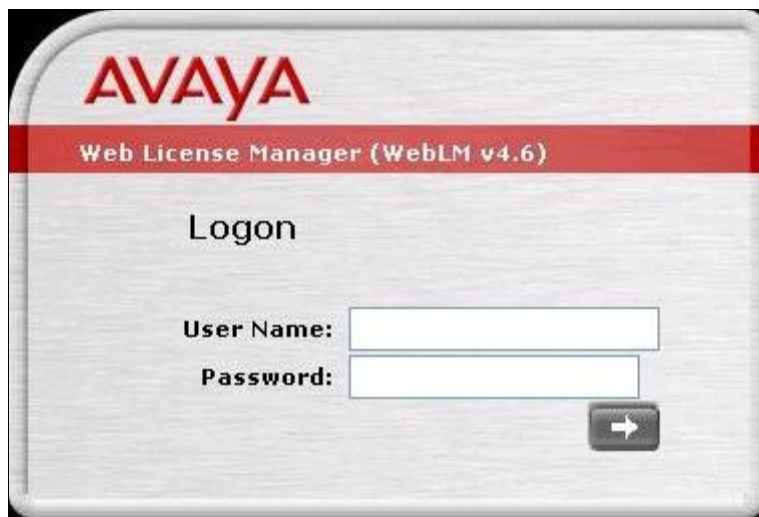
This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures include the following areas:

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

6.1. 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**, as shown below.


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: 6 - SID: 10503000 (Standard License File)

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

License installed on: Apr 18, 2011 4:49:38 PM EDT

[View Peak Usage](#)

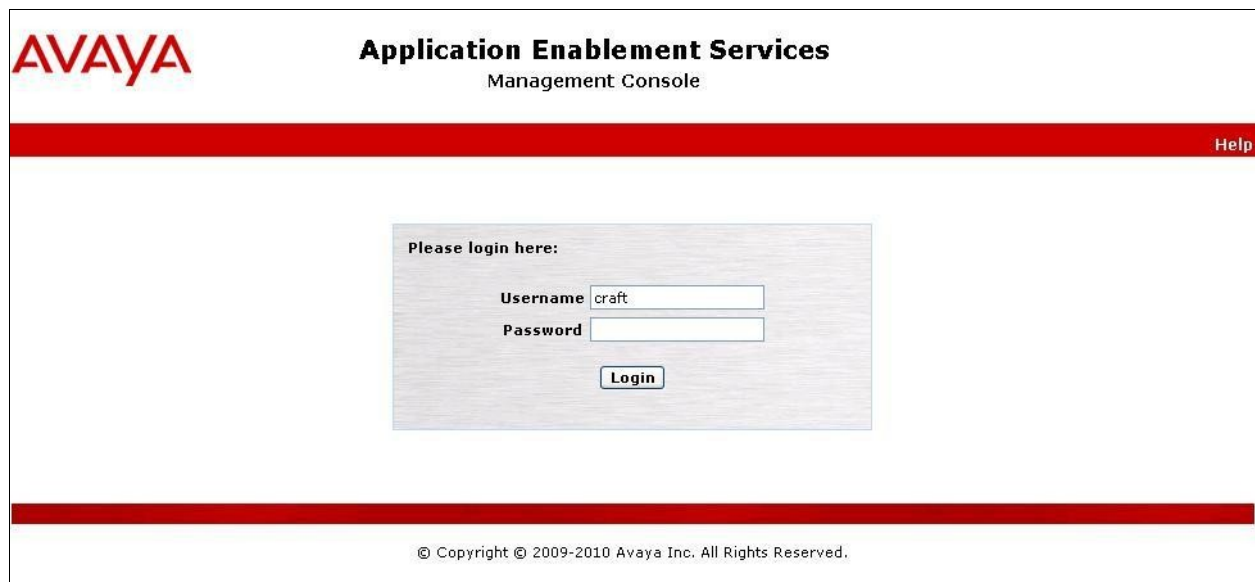
Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	2011/10/15	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	2011/10/15	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	2011/10/15	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	2011/10/15	16	0
Product Notes (VALUE_NOTES)	2011/10/15	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVIRINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	2011/10/15	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	2011/10/15	1000	0
DLG (VALUE_AES_DLG)	2011/10/15	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	2011/10/15	1000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	2011/10/15	3	0

6.2. 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 AVAYA Application Enablement Services Management Console login interface. At the top left is the AVAYA logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar at the top right contains a "Help" link. The main content area features a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. The "Username" field contains the text "craft". Below the input fields is a "Login" button. At the bottom of the page, a copyright notice reads: "© Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

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



The screenshot shows the AVAYA Application Enablement Services Management Console "Welcome to OAM" screen. At the top left is the AVAYA logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. In the top right corner, a welcome message is shown: "Welcome: User craft", "Last login: Fri Jun 24 14:31:29 2011 from 10.32.35.10", "HostName/IP: AES2-S8800/10.32.32.66", "Server Offer Type: VIRTUAL_APPLIANCE", and "SW Version: r6-1-0-20-0". A red horizontal bar below the header contains "Home" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical navigation menu with the following items: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains the following text: "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, a paragraph states: "Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain."

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.

6.3. 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 “S8800”, 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 is titled 'Switch Connections' and contains a table with the following data:

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8800	No	30	0

Below the table are several buttons: 'Add Connection', 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The 'Edit H.323 Gatekeeper' button is highlighted.

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 - S8800' screen. The left navigation pane is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main content area is titled 'Edit H.323 Gatekeeper - S8800' and contains a form with the following fields and buttons:

- A text input field containing '10.32.32.12'.
- An 'Add Name or IP' button.
- A 'Name or IP Address' label.
- 'Delete IP' and 'Back' buttons.

6.4. 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. Uncheck **Enable SDB for DMCC Service**, and click **Apply Changes**.

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 "craft" with login details. A red navigation bar contains "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various system components, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below these options.

6.5. 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).

**Application Enablement Services**
Management Console

Welcome: User craft
Last login: Fri Jun 24 14:31:29 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

User Management | User Admin | Add UserHome | 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"/>

6.6. 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** sub-section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA

Application Enablement Services
Management Console

Welcome: User craft
Last login: Fri Jun 24 14:31:29 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ 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"/>

7. Configure Avaya Proactive Contact

This section provides the procedures for how to obtain the necessary Interoperable Object Reference (IOR) file and host name information that are required by Envision Centricity.

7.1. Obtain IOR File

Envision Centricity uses the Event Service interface from Avaya Proactive Contact to obtain real-time agent states and call status events. The Event Service is a service based on the Common Object Request Broker Architecture (CORBA), and supports client application connection via several methods. The IOR method is used by Envision Centricity.

As part of installation, a copy of the IOR file from the Avaya Proactive Contact server needs to be provided to the Envision Centricity implementation team, and the path to the file is shown below:

`/opt/avaya/services/data/ns_ior`

7.2. Obtain Host Name

Log in to the Linux shell of the Avaya Proactive Contact server. Use the “`uname -a`” command to obtain the host name, which will be used later to configure Envision Centricity. In the compliance testing, the host name of the Avaya Proactive Contact server is “`lzpds4b`”, as shown below.

```
$ uname -a
Linux lzpds4b 2.6.9-42.0.10.ELsmp #1 SMP Fri Feb 16 17:17:21 EST 2007 i686 athlon i386
GNU/Linux
LZPDS4B(admin)/opt/avaya/pds [4]
$
```

8. Configure Envision Centricity

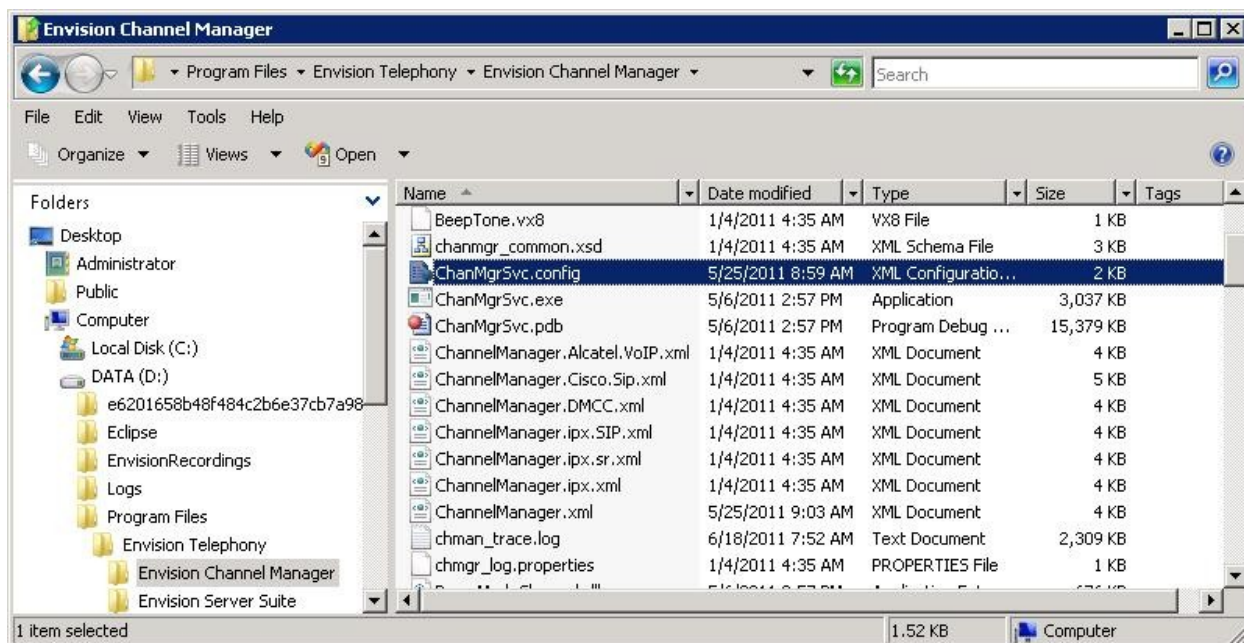
This section provides the procedures for configuring Envision Centricity. The procedures include the following areas:

- Administer ChanMgrSvc.config
- Administer ChannelManager.xml
- Launch Administrator
- Administer system settings
- Administer telephony settings
- Administer telephony PDS
- Administer telephony Envision servers
- Administer telephony device IDs
- Administer telephony ACD 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.

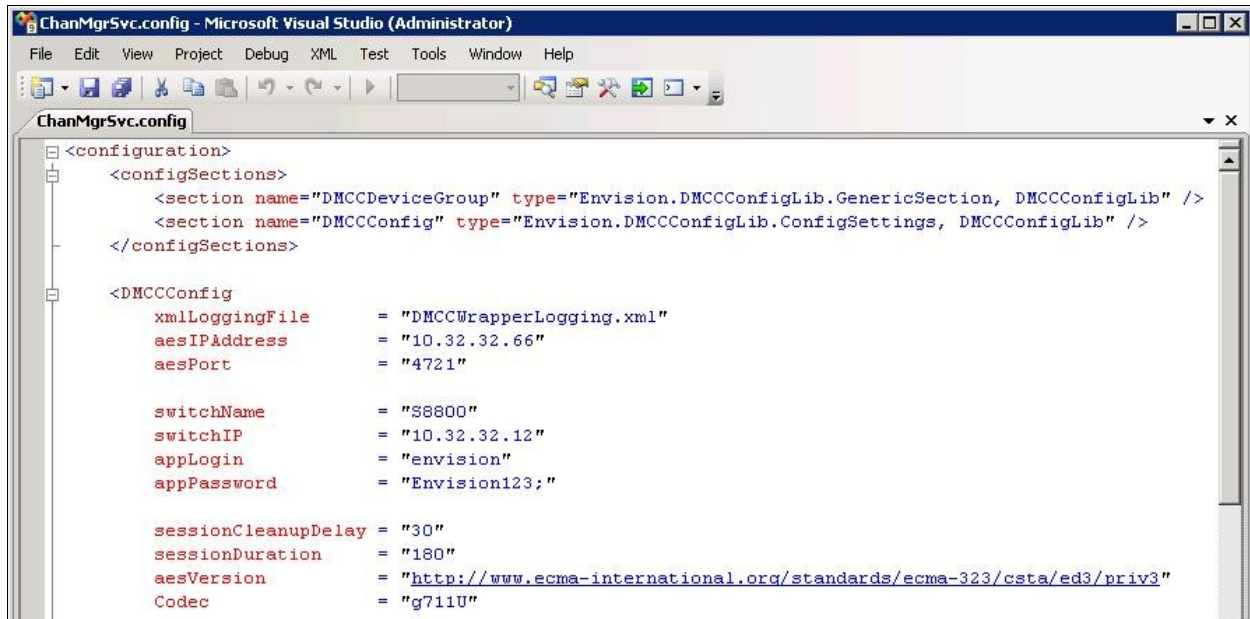
8.1. Administer ChanMgrSvc.config

From the Centricity server, navigate to the **D:\Program Files\Envision Telephony\ Envision Channel Manager** directory to locate the **ChanMgrSvc.config** file shown below.



Open the **ChanMgrSvc.config** file with the desired 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 6.3**.
- **switchIP:** IP address of the H.323 gatekeeper from **Section 6.3**.
- **appLogin:** Envision user credentials from **Section 6.5**.
- **appPassword:** Envision user credentials from **Section 6.5**.



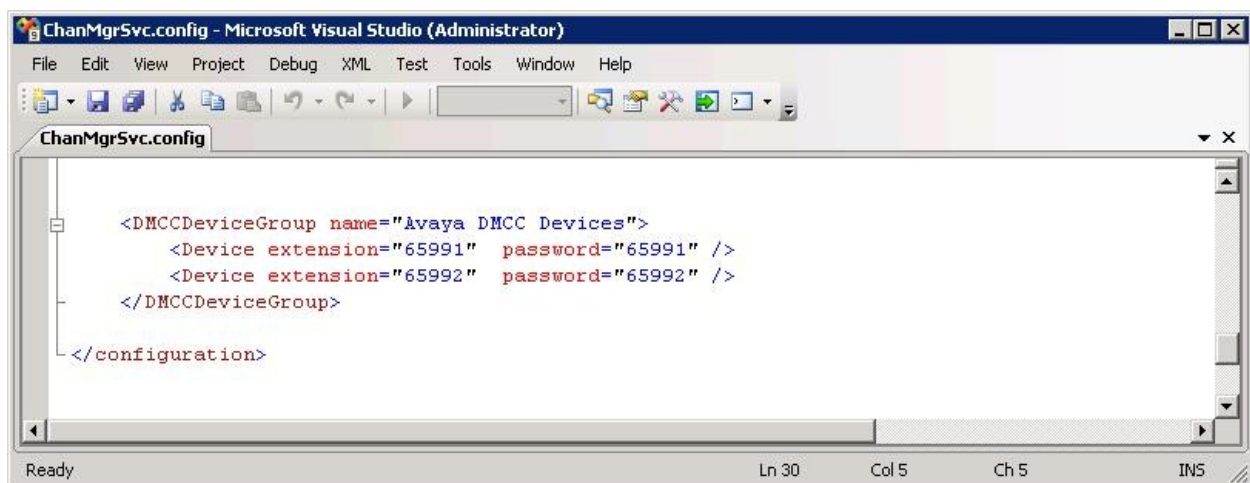
```
<configuration>
  <configSections>
    <section name="DMCCDeviceGroup" type="Envision.DMCCConfigLib.GenericSection, DMCCConfigLib" />
    <section name="DMCCConfig" type="Envision.DMCCConfigLib.ConfigSettings, DMCCConfigLib" />
  </configSections>

  <DMCCConfig
    xmlLoggingFile      = "DMCCWrapperLogging.xml"
    aesIPAddress        = "10.32.32.66"
    aesPort             = "4721"

    switchName          = "S8800"
    switchIP            = "10.32.32.12"
    appLogin            = "envision"
    appPassword         = "Envision123;"

    sessionCleanupDelay = "30"
    sessionDuration     = "180"
    aesVersion          = "http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv3"
    Codec               = "g711U"
  </DMCCConfig>
</configuration>
```

Scroll down to the **DMCCDeviceGroup** sub-section, and create an entry line with the extension and password for each virtual IP softphone from **Section 5.4**, as shown below.



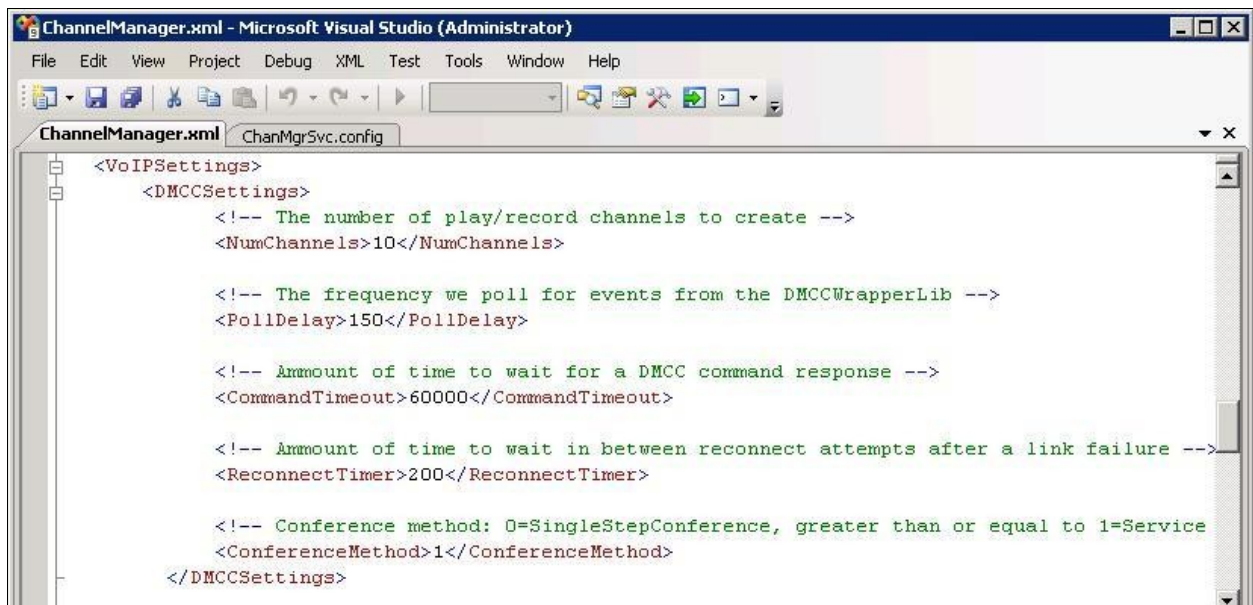
```
<DMCCDeviceGroup name="Avaya DMCC Devices">
  <Device extension="65991" password="65991" />
  <Device extension="65992" password="65992" />
</DMCCDeviceGroup>

</configuration>
```

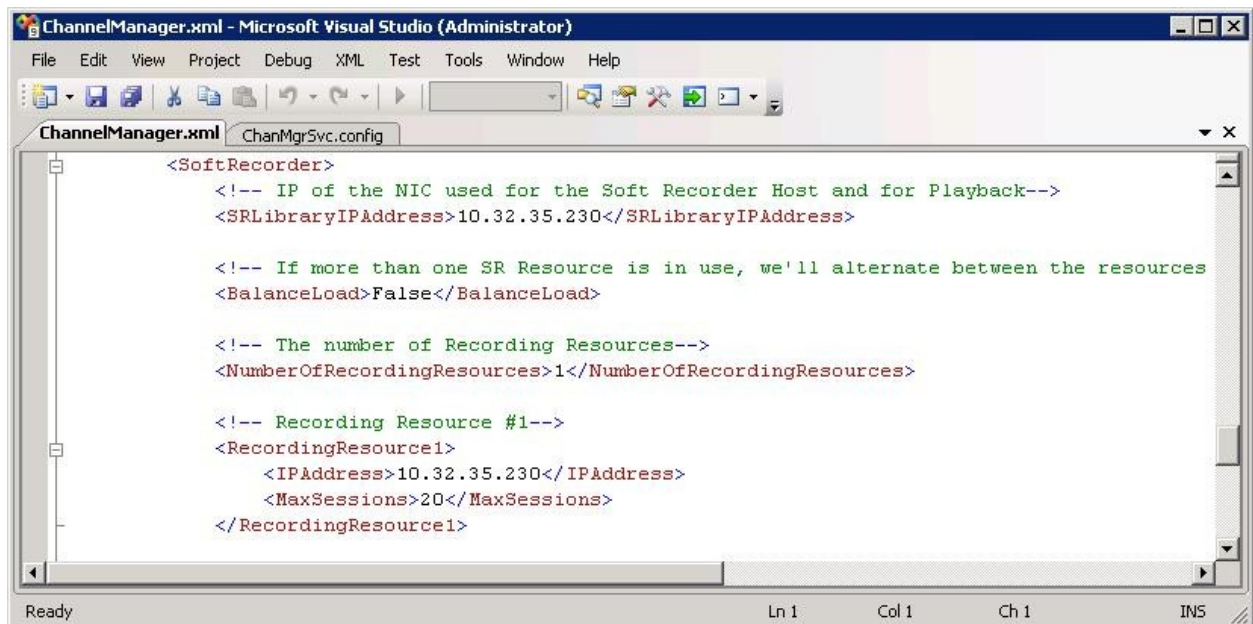
8.2. Administer ChannelManager.xml

From the same **D:\Program Files\Envision Telephony\Envision Channel Manager** directory, open the **ChannelManager.xml** file with the desired application.

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



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



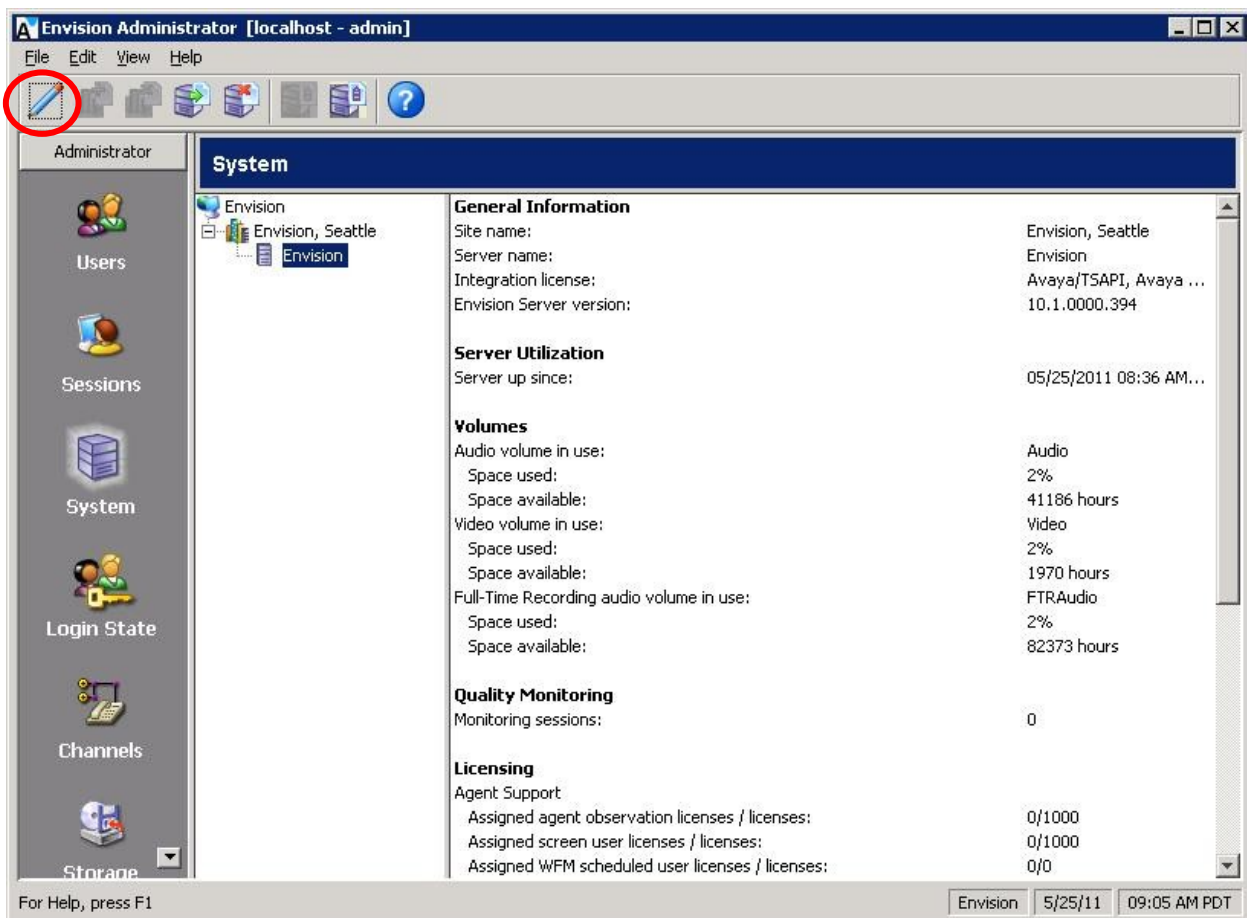
8.3. Launch Administrator

From the Centricity 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.



The image shows the 'Envision Administrator Login' dialog box. It has a title bar with the text 'Envision Administrator Login' and a close button. The dialog contains three input fields: 'User name:' with the text 'admin', 'Password:', and 'Server:' with a dropdown menu showing 'localhost'. There is a checkbox labeled 'Remember name and server.' which is checked. At the bottom right are 'OK' and 'Cancel' buttons. An illustration of a computer and server is on the right side of the dialog.

The **Envision Administrator** screen is displayed. Click the **Edit system settings** icon, as shown below.



The image shows the main window of the 'Envision Administrator' application. The title bar reads 'Envision Administrator [localhost - admin]'. The menu bar includes 'File', 'Edit', 'View', and 'Help'. The toolbar contains several icons, with the 'Edit system settings' icon (a pencil) circled in red. The left sidebar has a tree view with 'Administrator' selected, and sub-items: 'Users', 'Sessions', 'System', 'Login State', 'Channels', and 'Storage'. The main pane is titled 'System' and displays 'General Information', 'Server Utilization', 'Volumes', 'Quality Monitoring', and 'Licensing' sections. The status bar at the bottom shows 'For Help, press F1' on the left and 'Envision 5/25/11 09:05 AM PDT' on the right.

General Information	
Site name:	Envision, Seattle
Server name:	Envision
Integration license:	Avaya/TSAPI, Avaya ...
Envision Server version:	10.1.0000.394

Server Utilization	
Server up since:	05/25/2011 08:36 AM...

Volumes	
Audio volume in use:	Audio
Space used:	2%
Space available:	41186 hours
Video volume in use:	Video
Space used:	2%
Space available:	1970 hours
Full-Time Recording audio volume in use:	FTRAudio
Space used:	2%
Space available:	82373 hours

Quality Monitoring	
Monitoring sessions:	0

Licensing	
Agent Support	
Assigned agent observation licenses / licenses:	0/1000
Assigned screen user licenses / licenses:	0/1000
Assigned WFM scheduled user licenses / licenses:	0/0

8.4. 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 5.4**.

The screenshot shows the 'Edit server system settings' dialog box. The left pane has 'Channels' selected. The main area contains the following settings:

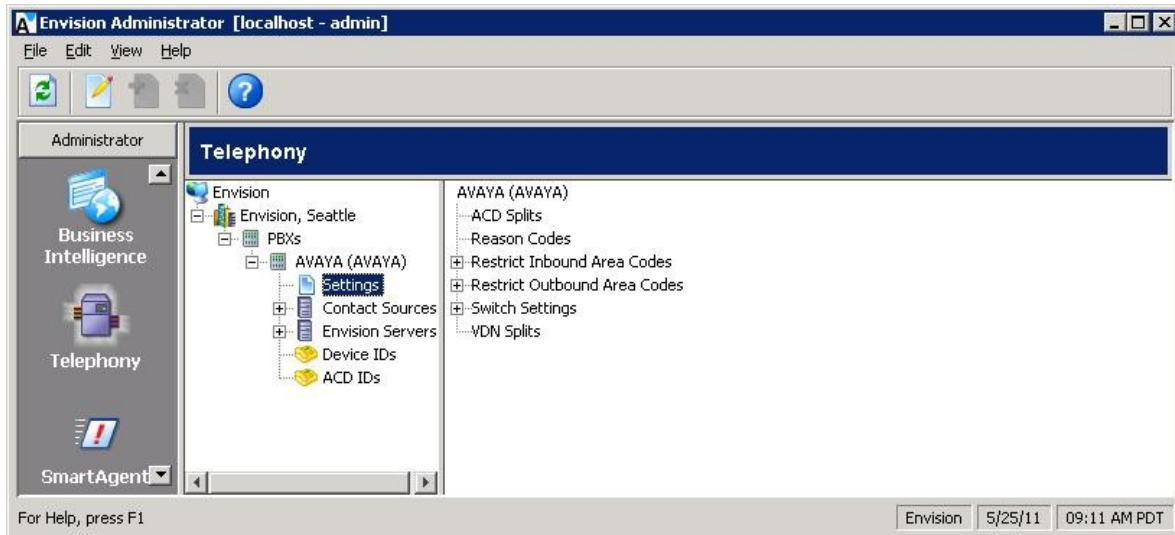
- * On new channel type install edit ChannelManager.xml
- On demand limit for agent observe channel: 1024
- Schedule limit for agent observe channel: 1024
- Release channel after disconnect: 2000 milliseconds
- Wait before sending service observe key code: 0 milliseconds
- Wait before observing agent: 0 milliseconds
- Wait before dialing: 0 milliseconds
- Custom Service Observe key code: 4
- State Transition File: D:\Program Files\Envision Telephc
- Event Data File: D:\Program Files\Envision Telephc
- Channel Manager Server: localhost
- Channel Manager Port: 59991
- AudioCodes Channels
 - Silence event after: 1000 milliseconds
 - Maximum silence event after: 30000 milliseconds
 - Activity event after: 100 milliseconds
 - Maximum activity event after: 10000 milliseconds

Buttons at the bottom: OK, Cancel, Apply.

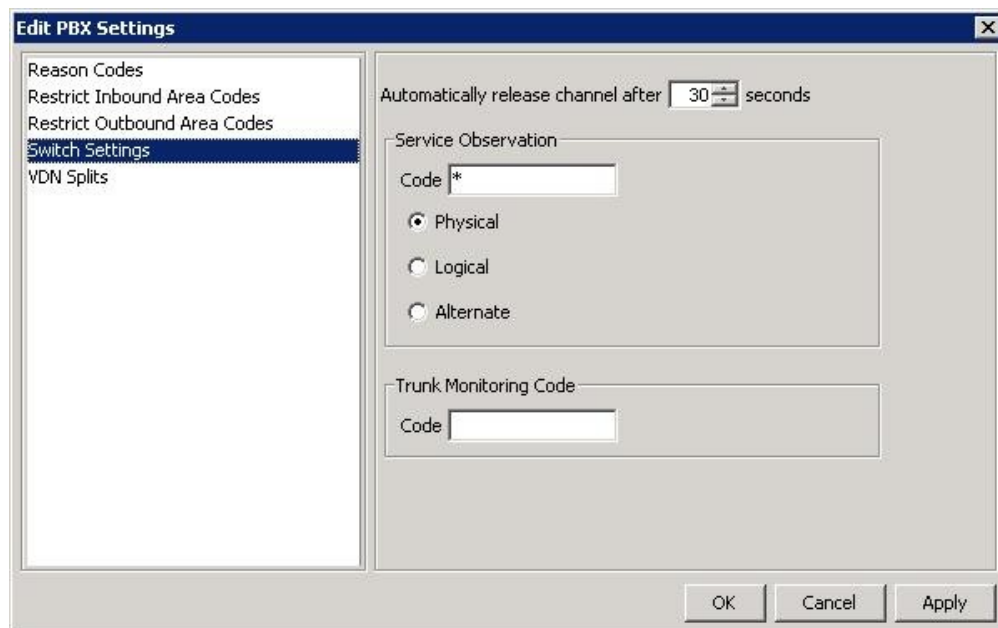
8.5. Administer Telephony Settings

The **Envision Administrator** screen is displayed again. Scroll 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 next. Select **Switch Settings** from the left pane. For **Service Observation Code**, enter a non-blank value. Retain the default values in the remaining fields.



8.6. Administer Telephony PDS

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



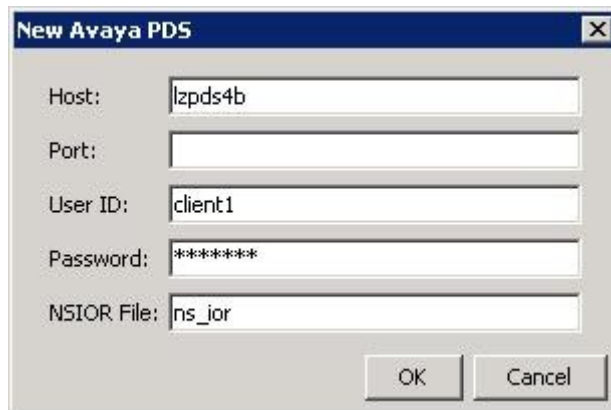
The **Add Contact Source** screen is displayed. Enter a descriptive **Name**. Select “Avaya PDS” as **Contact Source Type**, and click **OK**.



The **New Avaya PDS** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Host:** The host name of Avaya Proactive Contact from **Section 7.2**.
- **User ID:** The name of the Avaya Proactive Contact Event Service client.
- **Password:** The password of the Avaya Proactive Contact Event Service client.
- **NSIOR File:** The name of the IOR file.

Note that the IOR file was manually obtained from Avaya Proactive Contact, and placed in the default location of **D:\Program Files\Envision Telephony\Envision Server Suite\ContactSourceRunner**.



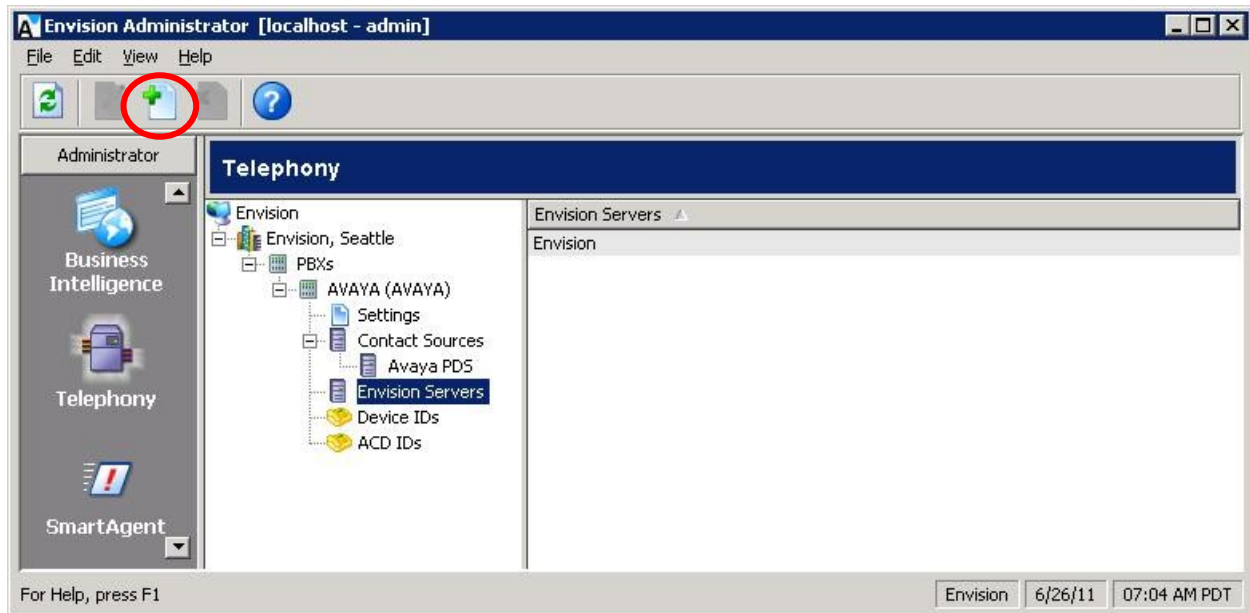
The screenshot shows a Windows-style dialog box titled "New Avaya PDS". It contains the following fields and values:

Field	Value
Host:	lpds4b
Port:	
User ID:	client1
Password:	*****
NSIOR File:	ns_ior

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

8.7. Administer Telephony Envision Servers

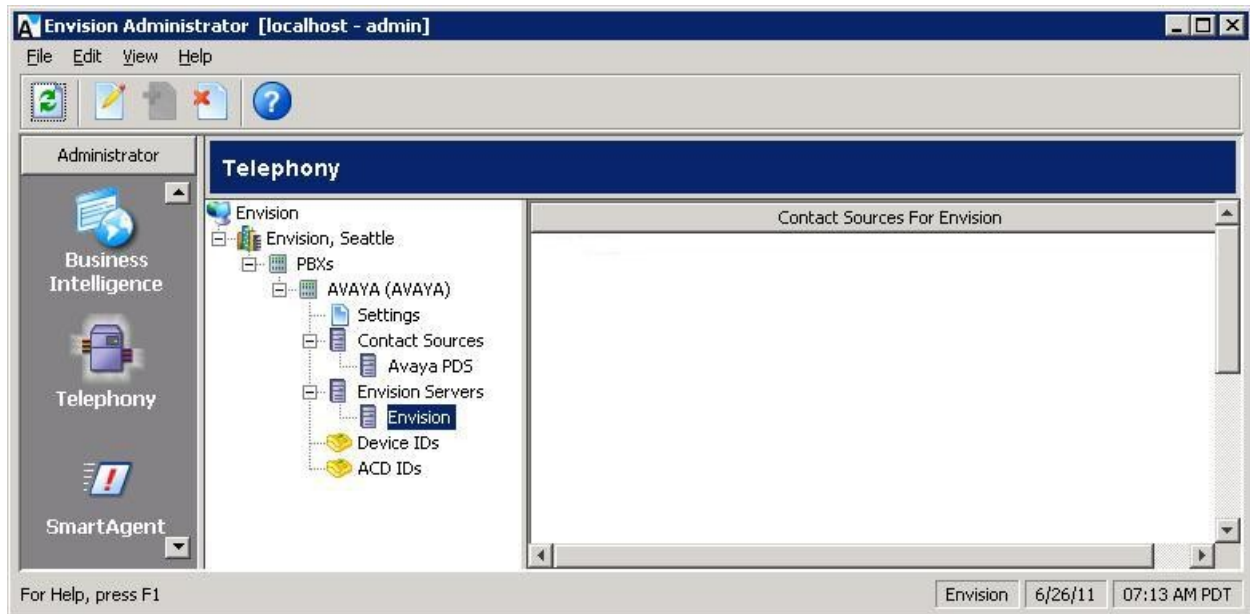
The **Telephony** screen is displayed again. Select **Envision > Envision, Seattle > PBXs > AVAYA (AVAYA) > Envision Servers** in the middle pane, and click the **New telephony setting** icon shown below.



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



Select the newly added Envision server in the middle pane. Right click in the right pane and select **New** (not shown).

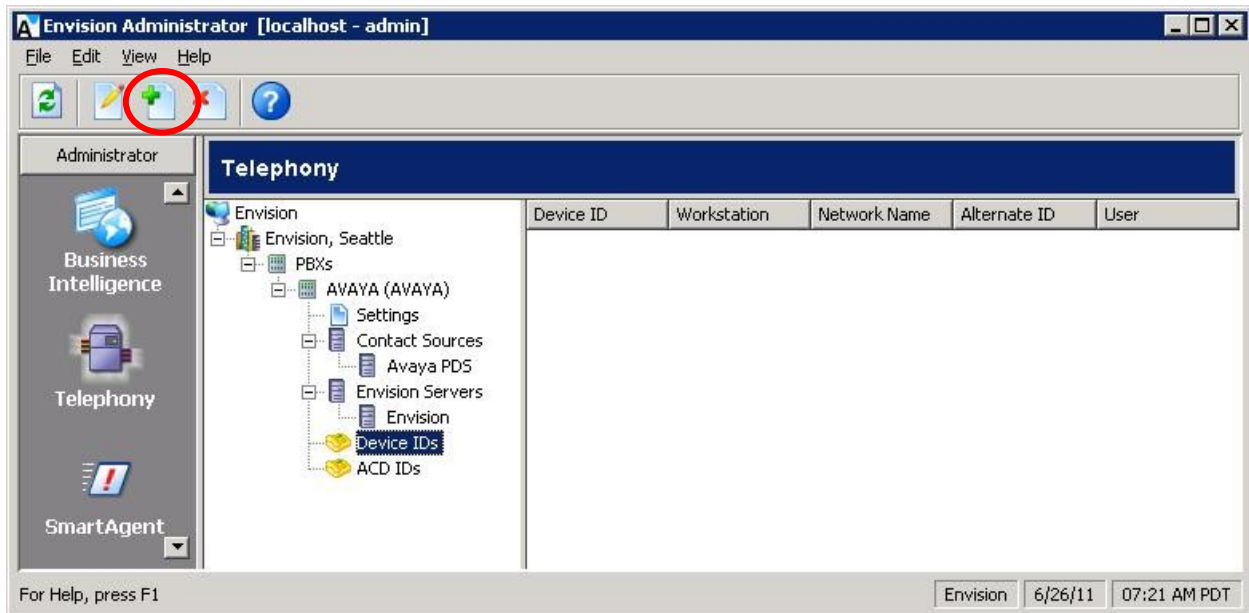


The **Assign Contact Source to Server** screen is displayed. Select the PDS contact source from **Section 8.6**, as shown below.



8.8. 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.

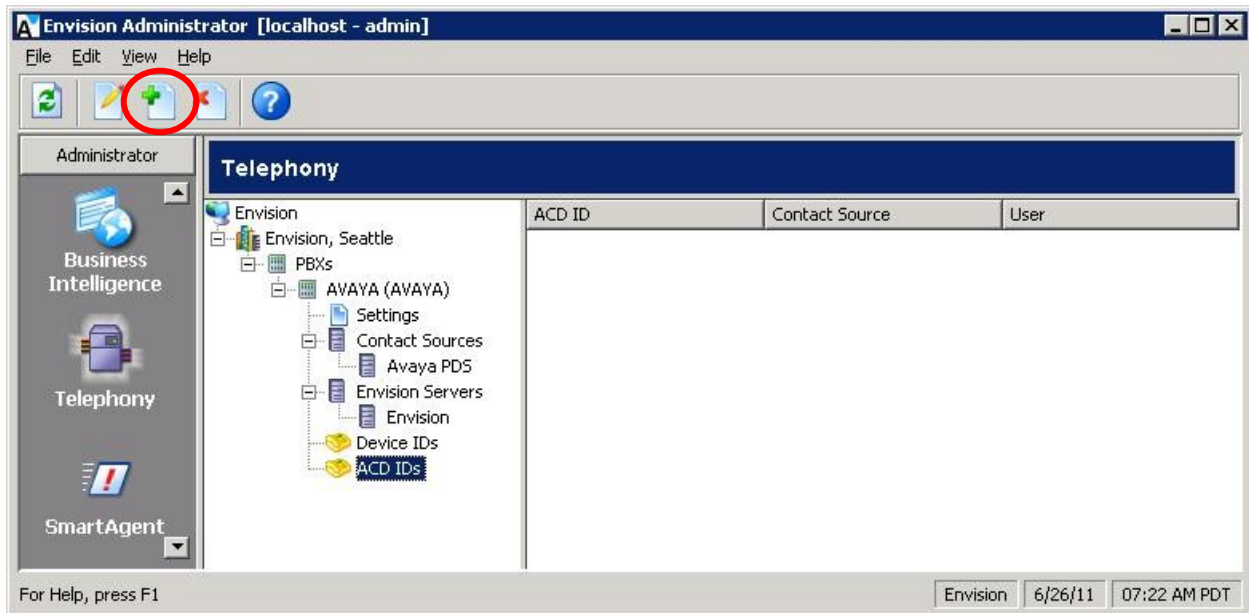


The **Add Device IDs** screen is displayed. Create a device ID for each agent station from **Section 3**. Note that ranges can be used for consecutive agent stations, as shown below.

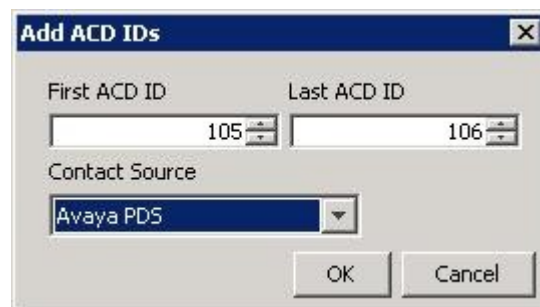
First Device ID		Last Device ID	
65001		65002	
Workstation		Network Name	
<input type="checkbox"/> Alternate ID			
		1	
OK		Cancel	

8.9. Administer Telephony ACD IDs

The **Telephony** screen is displayed again. Select **Envision > Envision, Seattle > PBXs > AVAYA (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 ID from **Section 3**, and select the PDS contact source from **Section 8.6** as the **Contact Source**. Note that ranges can be used for consecutive agent IDs, as shown below.



8.10. 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 3**. Enter a desired **User name** and **Full name**. Select the proper **Device ID** and **ACD ID**, and retain the default values in the remaining fields.

General | Privileges | Assignments | Agent components | View | Certificates

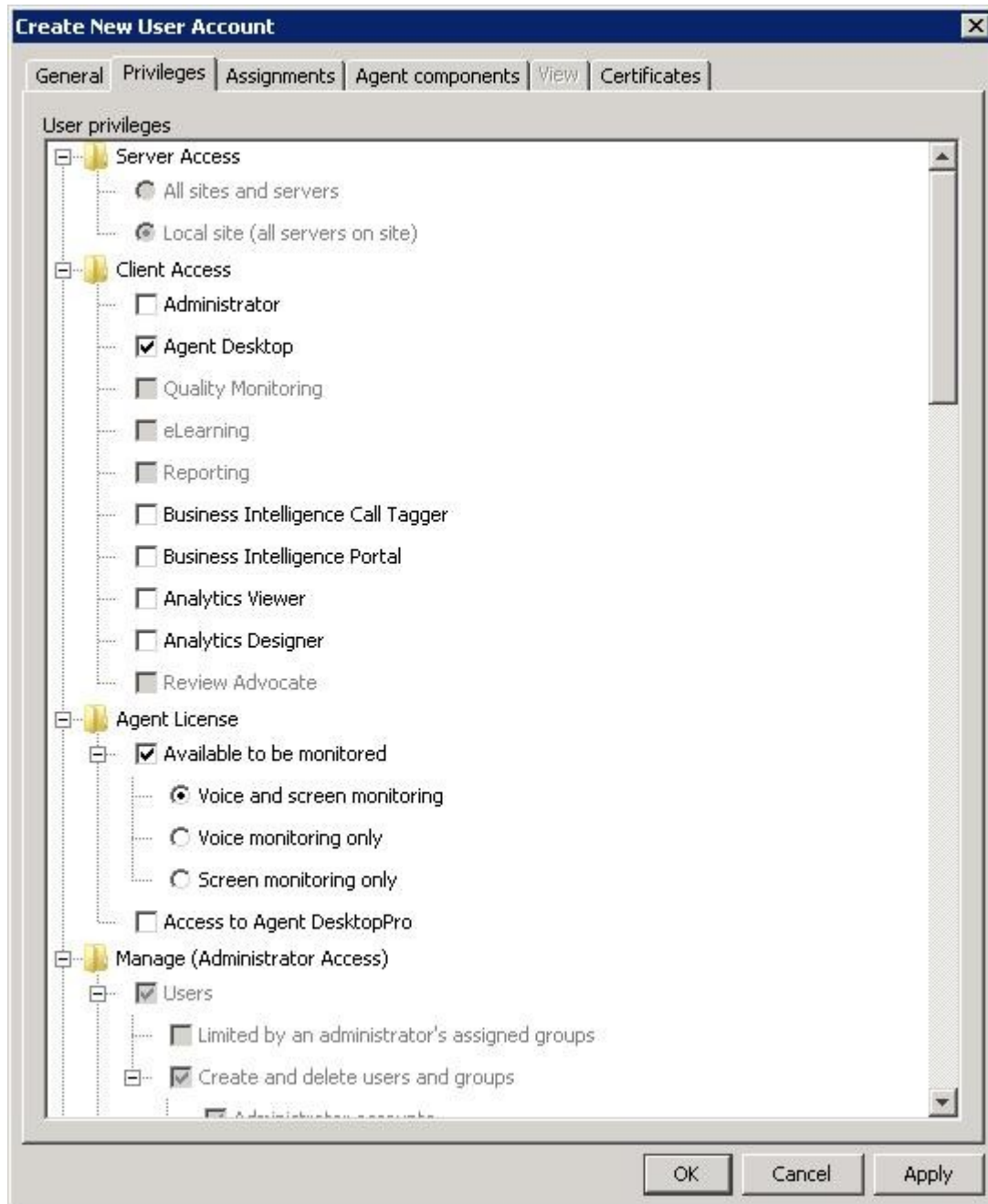
Domain name:
Network login name:
User name *:
Full name *:
Change password...
* Required Field

PBX:
Device ID:
ACD ID: ☒ 105 ☐ 106

Account:
☐ Inactive
☒ Active
☐ Active until:
Calendar: Jun 2011
S M T W T F S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30

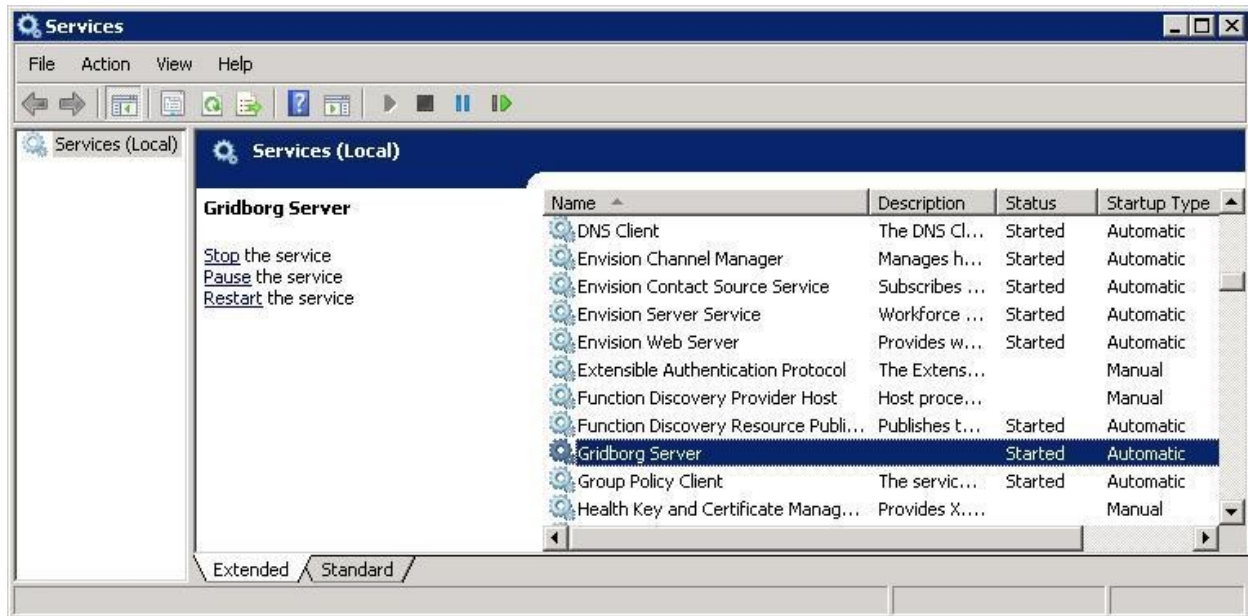
OK Cancel Apply

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.



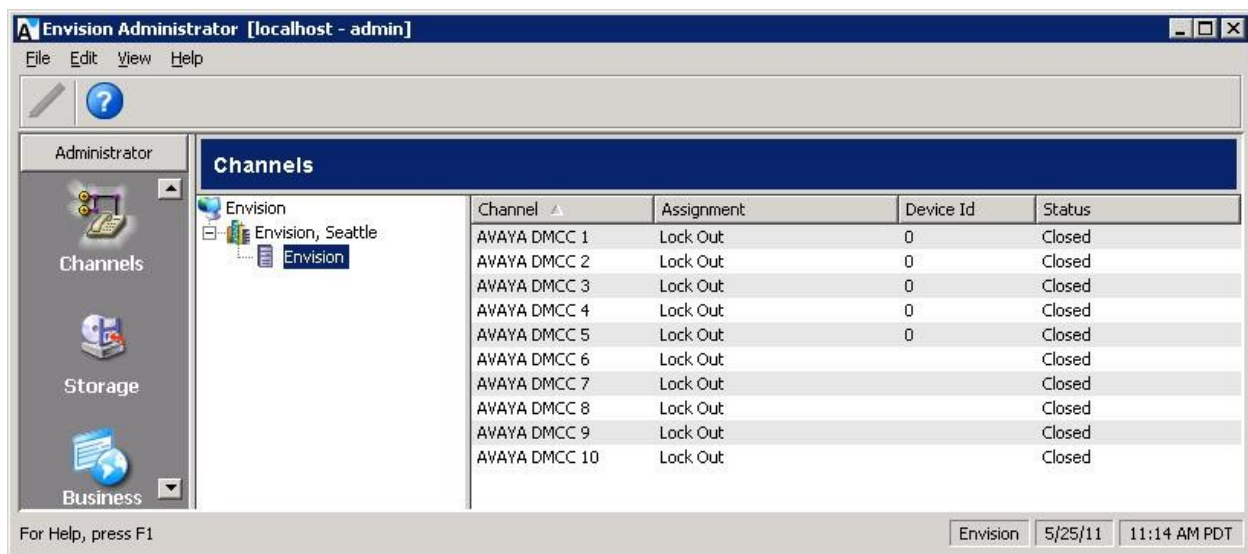
8.11. Restart Services

From the Envision server, select **Start > All Programs > Administrative Tools > Services** to display the **Services (Local)** screen. Restart the **SRMon Service** (not shown) and **Gridborg Server**, followed by **Envision Channel Manager**, **Envision Contact Source Service**, and **Envision Server Service**.



8.12. 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 “Agent Observe”. Repeat this section for the applicable channels. In the compliance testing, DMCC channels 1 and 2 were configured.

Administer channels

Channel

- AVAYA DMCC 1
- AVAYA DMCC 2
- AVAYA DMCC 3
- AVAYA DMCC 4
- AVAYA DMCC 5
- AVAYA DMCC 6
- AVAYA DMCC 7
- AVAYA DMCC 8
- AVAYA DMCC 9
- AVAYA DMCC 10

Select a channel in the list. Then, select a channel assignment and enter a device Id.

Assignment: Agent Observe

Device Id: 0

OK Cancel Apply

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration.

Prior to verification, follow [5] to use the Envision Quality Monitoring application to create recording schedules for agents. In the compliance testing, a non-recurring schedule was created for both agents to enable call recording for the current week.

9.1. Verify Avaya Aura® 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 6.5**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes 'Status | Status and Control | DMCC Service Summary' and links for 'Home | Help | Logout'. The left sidebar lists various services, with 'Status' expanded to show 'Status and Control' and 'DMCC Service Summary' selected. The main content area displays the 'DMCC Service Summary - Session Summary' page. It includes a session summary table with columns for Session ID, User, Application, Far-end Identifier, Connection Type, and # of Associated Devices. The table shows one active session for user 'envision' with application 'S8800' and far-end identifier '10.32.35.230'. Below the table are buttons for 'Terminate Sessions' and 'Show Terminated Sessions'.

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
BBCB95ECBBEEC85D0 65A78BDF81DADBA-23	envision	S8800	10.32.35.230	XML Unencrypted	0

9.2. Verify Avaya Proactive Contact

Log in to the Linux shell of the Avaya Proactive Contact server, and issue the “netstat | grep ensERVER” command. Verify that there is an entry showing an **ESTABLISHED** connection between the Avaya Proactive Contact Event Server and Envision Centricity, as shown below.

```

tcp        0      0 1zpds4b:enserver_ssl      1zpds4b:43283      ESTABLISHED
tcp        0      0 1zpds4b:enserver_ssl      10.32.35.230:57094  ESTABLISHED
tcp        0      0 1zpds4b:43283             1zpds4b:enserver_ssl ESTABLISHED

```

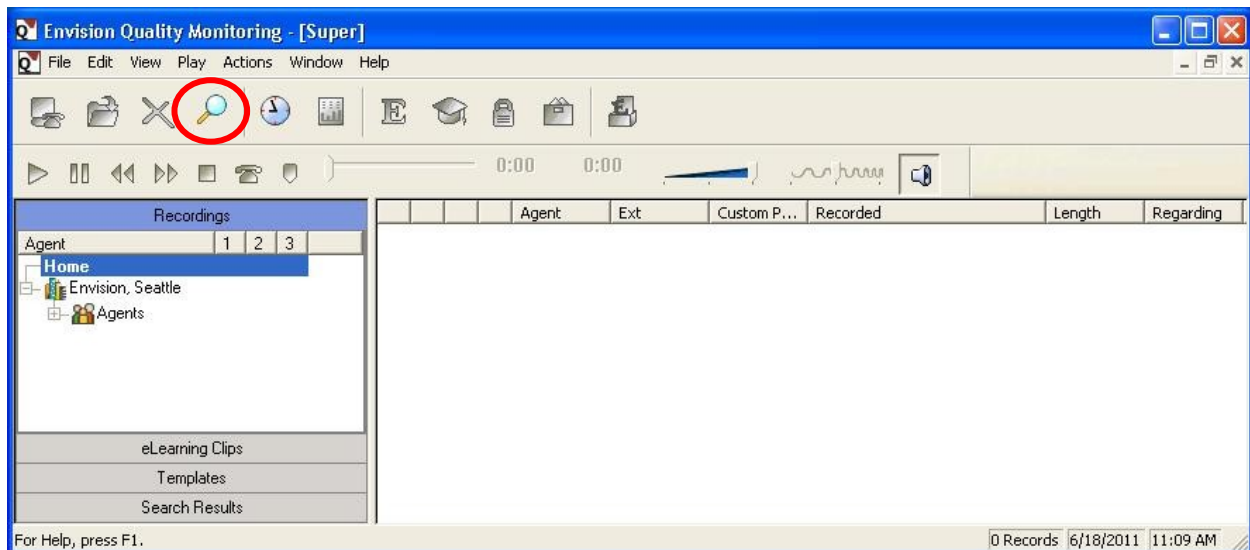
9.3. Verify Envision Centricity

Start a job on Avaya Proactive Contact, and log an agent in to handle and complete a call. From the supervisor PC, select **Start > Programs > Envision Telephony > Envision Performance Suite > Quality Monitoring** to launch the **Quality Monitoring** application.

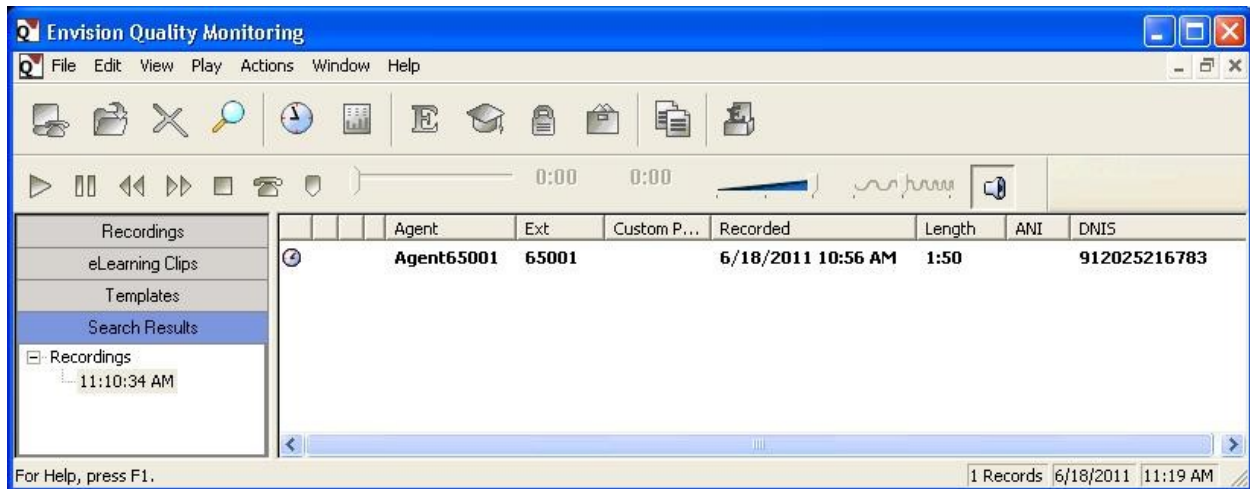
The **Envision Login** screen is displayed. For **Server**, select the IP address of the Centricity server. Enter the appropriate credentials.



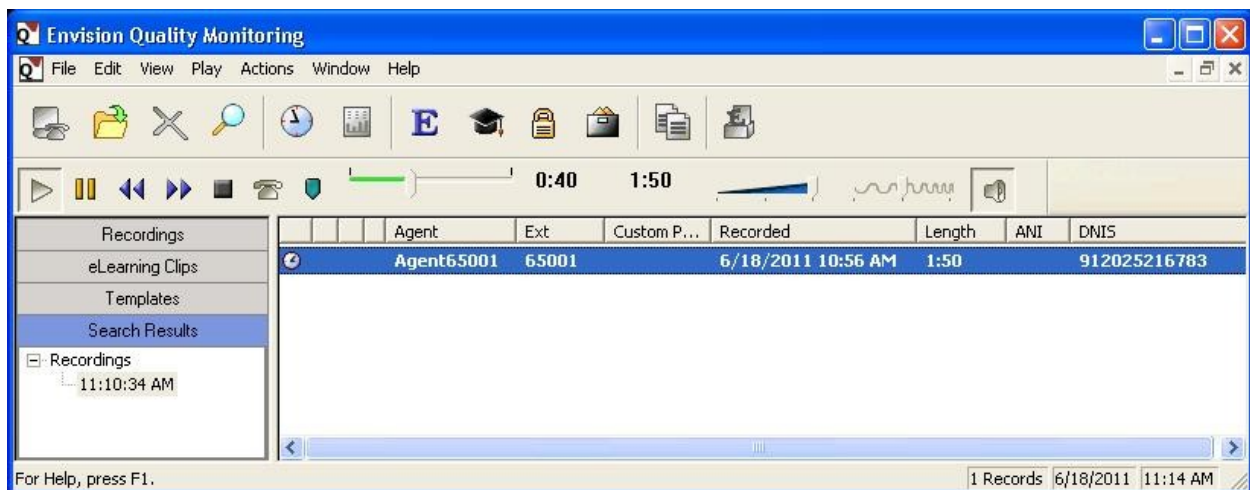
The **Envision Quality Monitoring** screen is displayed. Click on the **Search** icon shown below. The **Search for Recordings** screen is displayed next (not shown), retain all default values to enable search for all recordings for the current day.



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.



10. Conclusion

These Application Notes describe the configuration steps required for Envision Centricity to successfully interoperate with Avaya Proactive Contact with PG230 and Avaya Aura® Application Enablement Services for Quality Monitoring with Service Observing. All feature and serviceability test cases were completed with observations noted in **Section 2**.

11. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Administering Avaya Proactive Contact*, Release 4.2, May 2010, available at <http://support.avaya.com>.
3. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011, available at <http://support.avaya.com>.
4. *Envision Administrator Guide*, Version 10.1, available on the Envision server as part of installation.
5. *Envision Quality Monitoring User's Guide*, Version 10.1, available as part of the Envision Performance Suite installation.

©2011 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.