



Avaya Solution & Interoperability Test Lab

Application Notes for the DataVoice Recording Solution for Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the DataVoice Recording Solution for Avaya Communication Manager to monitor and record calls placed to and from stations on Avaya Communication Manager.

Recording start and stop decisions are made based on information received from the Telephony Services Application Programming Interface (TSAPI).

The DataVoice Recording Solution for Avaya Communication Manager can be configured to utilize the Device, Media and Call Control (DMCC) service to register DMCC softphones for use as recording ports using the TSAPI Single Step Conference (SSC) feature to conference in the recording device (DMCC station). Alternatively, the trunk tap recording method may be used. These Application Notes describe both recording configurations.

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 a compliance-tested configuration comprised of an Avaya Communication Manager, an Avaya Application Enablement Services (AES) server, and the DataVoice Recording Solution for Avaya Communication Manager.

The DataVoice Recording Solution for Avaya Communication Manager consists of two components:

- The DataVoice Avaya Communication Manager Recording Controller - The DataVoice Avaya Communication Manager (CM) Recording Controller connects to the Avaya Application Enablement Services (AES) server using the Telephony Services Application Programming Interface (TSAPI). The Recording Controller (RC) monitors extensions that must be recorded to obtain telephony call events which are used to start, stop and annotate recordings, and in general to control the DataVoice Libra Recorder (see following section). System setup and configuration for the Recording Controller is done through the DataVoice RC Setup and Recording Controller Configuration Utilities.
- The DataVoice Libra Recorder - The DataVoice Libra Recorder records user conversations in circuit-switched telephony (CST) and IP telephony environments. The Recorder uses indirect recording for circuit-switched and unencrypted IP telephony recording, and it uses integrated recording for circuit-switched and both unencrypted as well as encrypted IP telephony recording. The terms indirect recording and integrated recording are defined in the next few sections. System setup and configuration for the Recorder is done through the DataVoice AdminConsole. Users access recorded conversations on the Libra Recorder via the browser-based DataVoice WebRecall interface to search, view, play and e-mail conversations.

The DataVoice Recording Solution for Avaya Communication Manager supports two recording methods:

- Indirect Recording – When using Indirect Recording, there is no direct connection between the monitored device and the Recorder. The Recorder is connected to an E1/T1 Digital Trunk line. Only external calls can be recorded. External calls are calls that originate or terminate on the PSTN side of the PBX. This is also known as Trunk, Tap or CST recording.
- Integrated Recording – With Integrated Recording an internal connection between the monitored device and the Recorder is created via the switch at the time when the monitored device needs to be recorded. In this case, the Recording Controller is using the Single Step Conference CTI command to conference Recorder-hosted DMCC softphones into calls that must be recorded. This feature allows the Recording Controller to tap into a call without influencing the call in any way. The Recorder connects to the Avaya Application Enablement Services (AES) server using the Device, Media and Call Control (DMCC) interface. The Recorder monitors the dedicated DMCC softphones to

obtain the events which are used to capture the audio. This is also known as Call Monitoring or Silent Conference.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included during the test, to provide an IP trunk between two Avaya Communication Manager systems.

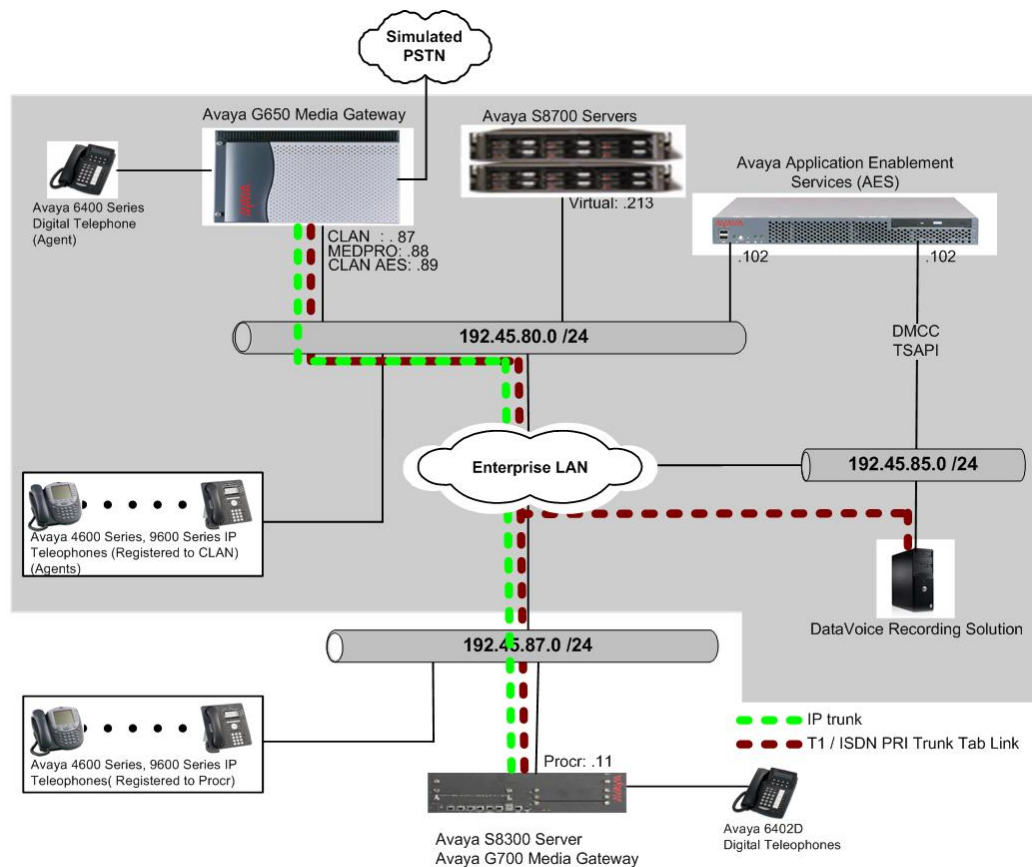


Figure 1: Sample Test Configuration for the DataVoice Solution

2. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8720 Server		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface	HW11 FW030
	TN799DP C-LAN Interface	HW20 FW017
	TN2302AP IP Media Processor	HW01 FW108
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya Application Enablement Services Server		4.2 (R4.2.0.19.4)
Avaya 4600 Series IP Telephones		
	4620SW (H.323)	2.8
	4625SW (H.323)	2.8
Avaya 9600 Series IP Telephones		
	9630 (H.323)	1.5
	9650 (H.323)	1.5
Avaya 6408D+ Digital Telephone		-
DataVoice Avaya Communication Manager Recording Controller		V3.6.0.20
Note: Operating System used was Microsoft Windows XP Professional Version 2002 with Service Pack 3		
DataVoice Libra Recorder		V5.0.0.23
Note: Operating System used was Microsoft Windows XP Professional Version 2002 with Service Pack 3		

3. Configure Avaya Communication Manager

This section provides the procedures for configuring an ip-codec-set and ip-network region, a switch connection and Computer Telephony Integration (CTI) links, monitored stations, and recording stations on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

3.1. Codec Configuration

Enter the **change ip-codec-set t** command, where **t** is a number between 1 and 7.

change ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size(ms)			
1:	G.711MU	n	2	20		

3.2. IP Network Regions

During compliance testing, a C-LAN board dedicated for H.323 endpoint registration was assigned to IP network region 1. The Avaya IP Telephones and IP Softphones, used by the DataVoice Recording Solution, registered with the C-LAN boards and were thus also assigned to IP network region 1. The second C-LAN board (CLAN-AES), which is dedicated for the AES server, was assigned to network region 2. The following screen shows only network region 1.

change ip-network-region 1		Page	1 of 19
IP NETWORK REGION			
Region: 1			
Location:		Authoritative Domain:	
Name:			
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 1		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048		IP Audio Hairpinning? n	
UDP Port Max: 3929			
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y	
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46		Use Default Server Parameters? y	
Video PHB Value: 46			
802.1P/Q PARAMETERS			
Call Control 802.1p Priority: 0			
Audio 802.1p Priority: 0			
Video 802.1p Priority: 5			
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 Link Bounce Recovery? y		RSVP Enabled? n	
Idle Traffic Interval (sec): 20			
Keep-Alive Interval (sec): 5			
Keep-Alive Count: 5			

3.3. Configure Switch Connection and CTI Links between Avaya Communication Manager and Avaya Application Enablement Services

The Avaya AES server forwards CTI requests, responses, and events between the DataVoice Avaya Communication Manager Recording Controller and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over a switch connection link. Within the switch connection link, CTI links may be configured to provide CTI services to CTI applications such as the DataVoice Recording Controller. The following steps demonstrate

the configuration of the Avaya Communication Manager side of the switch connection and CTI links. See **Section 4** for the details of configuring the AES side of the switch connection and CTI links.

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid extension under the provisioned dial plan in Avaya Communication Manager, set the Type field to **ADJ-IP**, and assign a descriptive Name to the CTI link.

add cti-link 4		Page 1 of 2
CTI LINK		
CTI Link: 4		
Extension: 20006		
Type: ADJ-IP		
COR: 1		
Name: TSAPI		

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoints (Avaya IP Telephones, and IP Softphones, and AES Device, Media and Call Control API stations) and the CLAN-AES IP address was used for connectivity to Avaya AES.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
CLAN	192.45.80.87	
CLAN-AES	192.45.80.89	
MEDPRO	192.45.80.88	
MEDPRO2	192.45.80.161	
S8300G700	192.45.87.11	
default	0.0.0.0	
procr	192.45.80.214	

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was utilized for the Local Port field.

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

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command **uname -a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in **Section 4.1**.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	server2	xxxxxxxxxxxxxxxxxx	y	idle
2:				
3:				

3.4. Monitored Stations

During the compliance test, the following recorded stations were used. These represent agent stations to be recorded.

- 22001 (Avaya 4620SW IP)
- 22002 (Avaya 4625SW IP)
- 22003 (Avaya 9630 IP)
- 22007 (Avaya 6408D+)
- 22009 (Avaya IP Agent)

3.5. DMCC Softphones

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, specify the Security Code, and make sure that the IP Softphone field is set to **y**. For the compliance test, DMCC softphones from 23001 to 23030 were created for integrated recording.

add station 23001		Page 1 of 5
STATION		
Extension: 23001	Lock Messages? n	BCC: 0
Type: 4620	Security Code: *	TN: 1
Port: S00046	Coverage Path 1:	COR: 1
Name: DMCC-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: 23001	
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	

4. Configure Avaya Application Enablement Services

The Avaya Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, the Avaya Application Enablement Services (AES) server receives responses and events from Avaya Communication Manager and forwards them to the appropriate CTI applications.

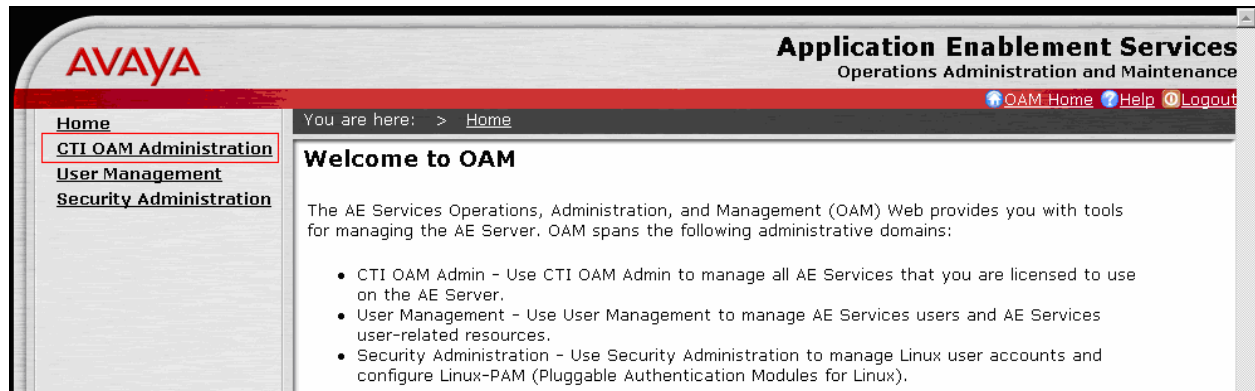
This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a DMCC Server port, and a CTI link for TSAPI.

4.1. Configure Switch Connection

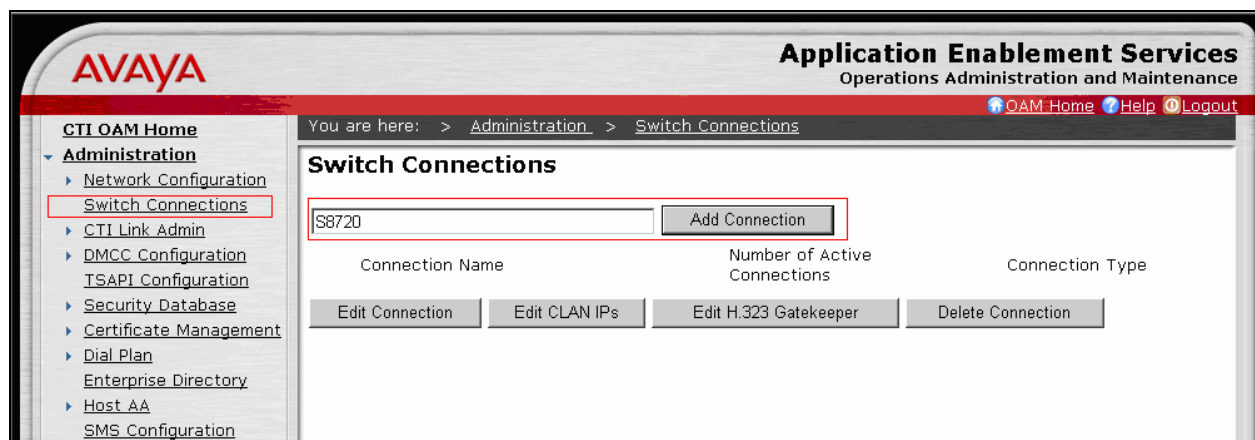
Launch a web browser, enter <http://<IP address of AES server>> in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.



Select the **CTI OAM Administration** link from the left pane of the screen.



Click on **Administration** → **Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in **Section 3.3**. Click on **Apply**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

Set Password - S8720

Please note the following:
* Changing the password affects only new connections, not open connections.

Switch Password:

Confirm Switch Password:

SSL: ☒

Apply **Cancel**

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

Switch Connections

Add Connection

Connection Name	Number of Active Connections
<input checked="" type="radio"/> S8720	0

Edit Connection **Edit CLAN IPs** **Edit H.323 Gatekeeper** **Delete Connection**

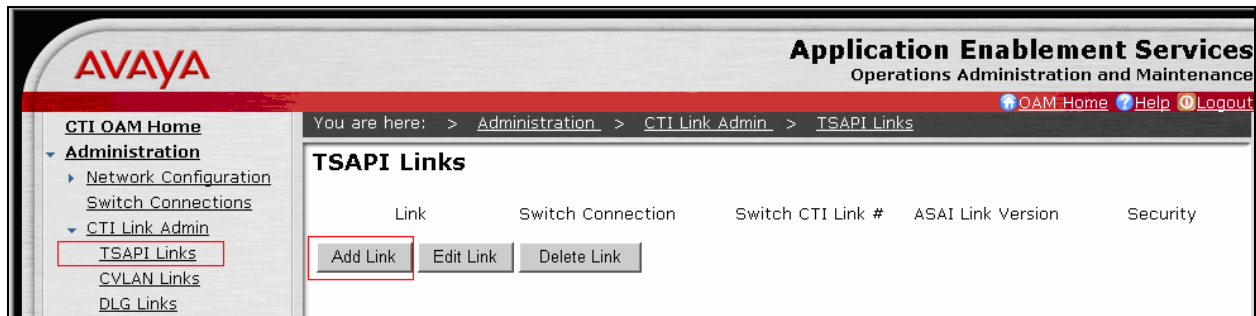
Enter the CLAN-AES IP address which was configured for AES connectivity in **Section 3.3** and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

After the completion, navigate back to **Administration** → **Switch Connections** in the left pane to invoke the Switch Connections page. Click on **Edit H.323 Gatekeeper** for DMCC call control and monitor.

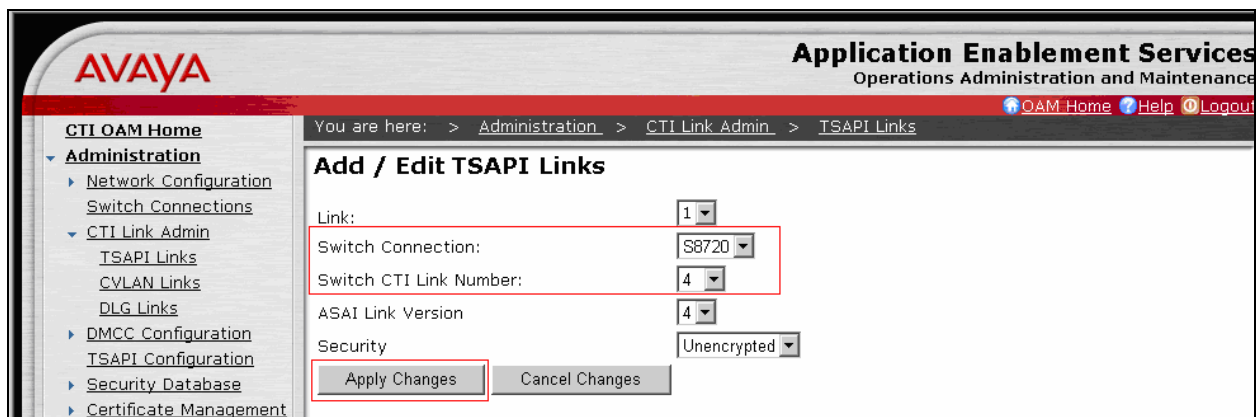
On the **Edit H.323 Gatekeeper – S8720** page, enter the C-LAN IP address which will be used for the DMCC service. During the compliance test, CLAN-AES was utilized for the DMCC service. Click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

4.2. Configure the TSAPI CTI link

Navigate to **Administration** → **CTI Link Admin** → **TSAPI Links** in the left pane, and click on the **Add Link** button to create a TSAPI CTI link.



Select a Switch Connection using the drop down menu. The Switch Connection is configured in **Section 4.1**. Select the Switch CTI Link Number using the drop down menu. The switch CTI Link Number should match the number configured in the cti-link form in **Section 3.3**. Click the **Apply Changes** button. Default values may be used in the remaining fields.

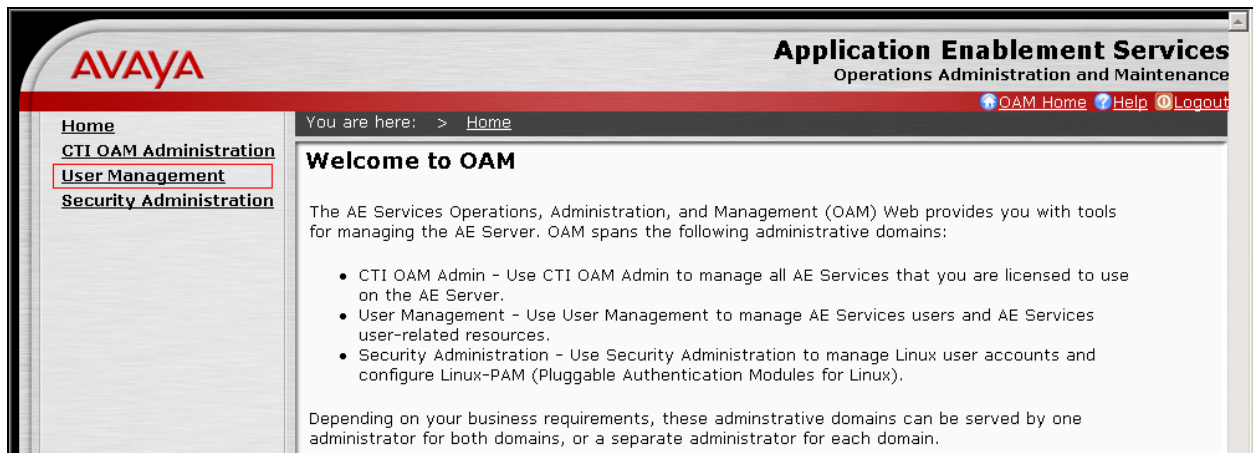


4.3. Configure the CTI Users

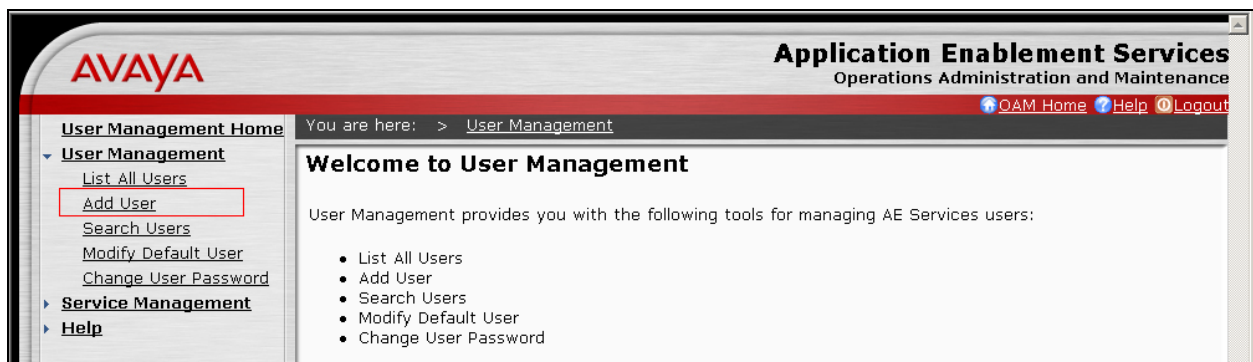
The steps in this section describe the configuration of a CTI user. Launch a web browser, enter <http://<IP address of AES server>> in the URL, and log in with the appropriate credentials to access the relevant administration pages.



The Welcome to OAM page is displayed next. Select **User Management** from the left pane.



From the Welcome to User Management page, navigate to the **User Management** → **Add User** page to add a CTI user.



On the Add User page, provide the following information:

- User Id
- Common Name
- Surname
- User Password
- Confirm Password

The above information (User ID and User Password) must match with the information configured in the DataVoice Configuration page in **Section 5**. Select **Yes** using the drop-down menu on the CT User field. This enables the user as a CTI user. Click the **Apply** button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > [User Management](#) > [Add User](#)

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

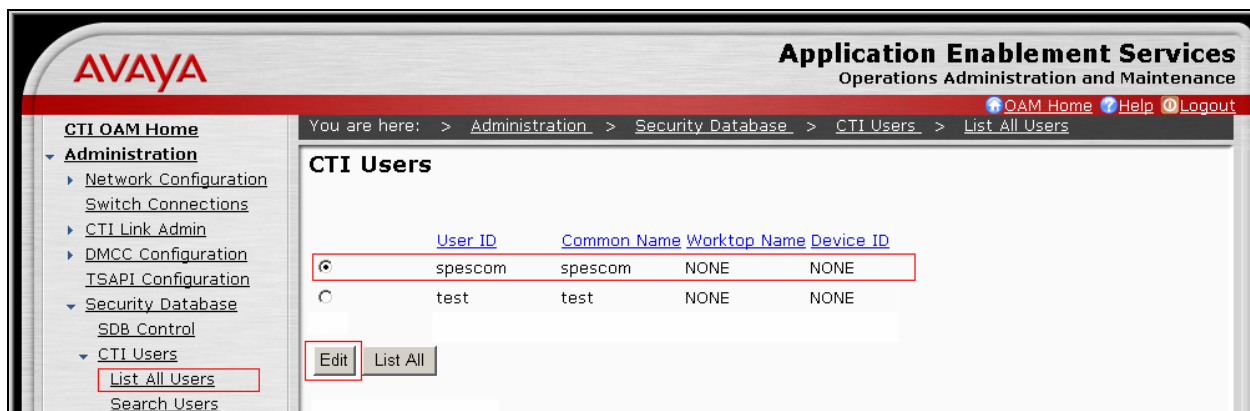
CT User

Department Number

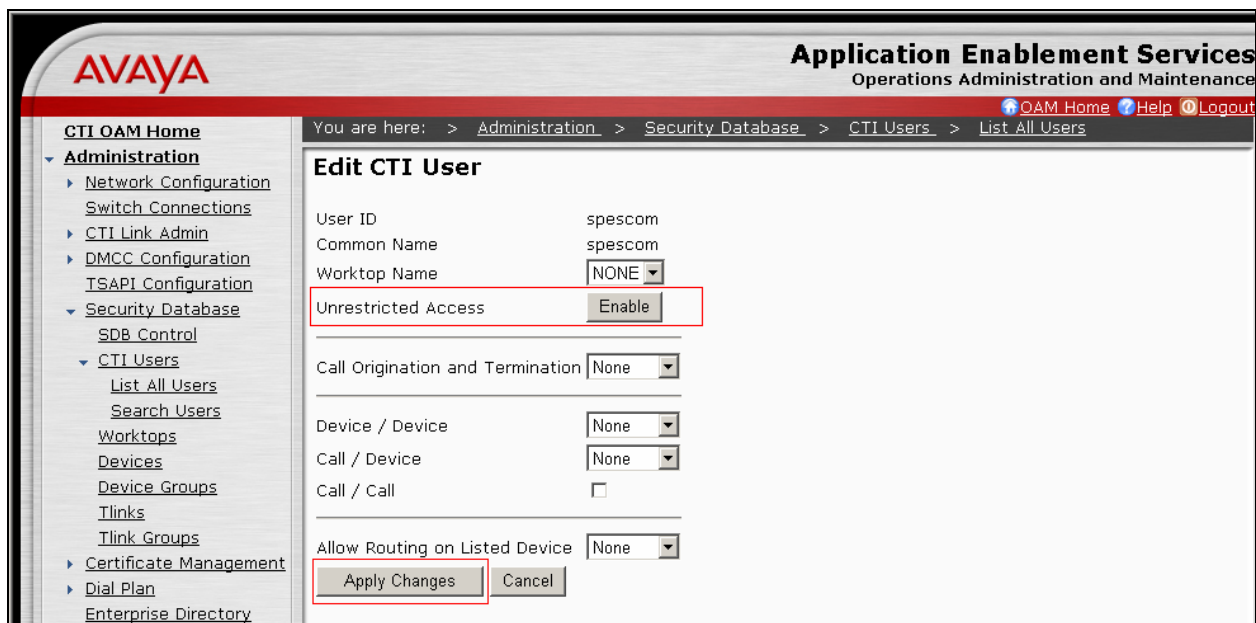
Display Name

Employee Number

Once the user is created, select **OAM Home** in upper right and navigate to the **CTI OAM Administration → Security Database → CTI Users → List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.



Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.



Navigate to the **CTI OAM Home** → **Administration** → **Ports** page to set the DMCC server port. During the compliance test, the default port values were used. The following screen displays the default port values. Since the encrypted port was used during the compliance test, set the Encrypted Port field to **Enabled**. Default values may be used in the remaining fields. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

AVAYA

Application Enablement Services

Operations Administration and Maintenance

CTI OAM Home

Administration

Network Configuration

Local IP

NIC Configuration

Ports

Switch Connections

CTI Link Admin

DMCC Configuration

TSAPI Configuration

Security Database

Certificate Management

Dial Plan

Enterprise Directory

Host AA

SMS Configuration

WebLM Configuration

Status and Control

Maintenance

Alarms

Logs

Utilities

Help

You are here: > Administration > Network Configuration > Ports

Ports

CVLAN Ports

Unencrypted TCP Port

9999

Enabled Disabled

Encrypted TCP Port

9998

Enabled Disabled

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port

450

Enabled Disabled

Local TLINK Ports

TCP Port Min

1024

TCP Port Max

1039

Unencrypted TLINK Ports

TCP Port Min

1050

TCP Port Max

1065

Encrypted TLINK Ports

TCP Port Min

1066

TCP Port Max

1081

DMCC Server Ports

Unencrypted Port

4721

Enabled Disabled

Encrypted Port

4722

Enabled Disabled

TR/87 Port

4723

Enabled Disabled

5. Configure DataVoice Recording Solution for Avaya Communication Manager

This section only describes the interface configuration that allows the DataVoice Avaya Communication Manager Recording Controller and DataVoice Libra Recorder to communicate with Avaya AES and Avaya Communication Manager.

Refer to [3] and [4] for instructions to configure the DataVoice Avaya Communication Manager Recording Controller and to [5] for configuring the DataVoice Libra Recorder.

5.1. Configure DataVoice Avaya Communication Manager Recording Controller

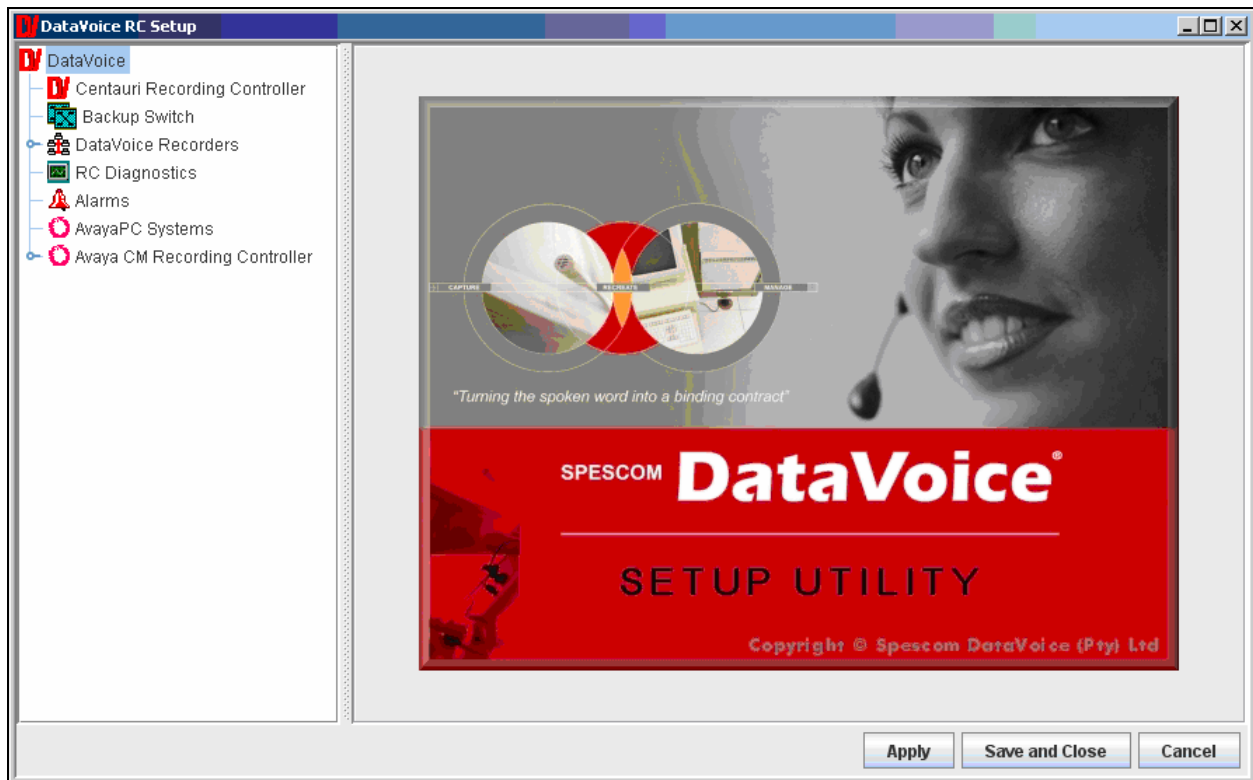
This section describes the setup of indirect and integrated recording for the Recording Controller.

The setup and configuration for the Recording Controller is done through the DataVoice RC Setup Utility. Open the DataVoice RC Setup Utility by double-clicking the **DV Setup** icon on the Windows Desktop.

CRK; Reviewed:
SPOC 12/15/2008

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

16 of 35
DataVoice-AES42



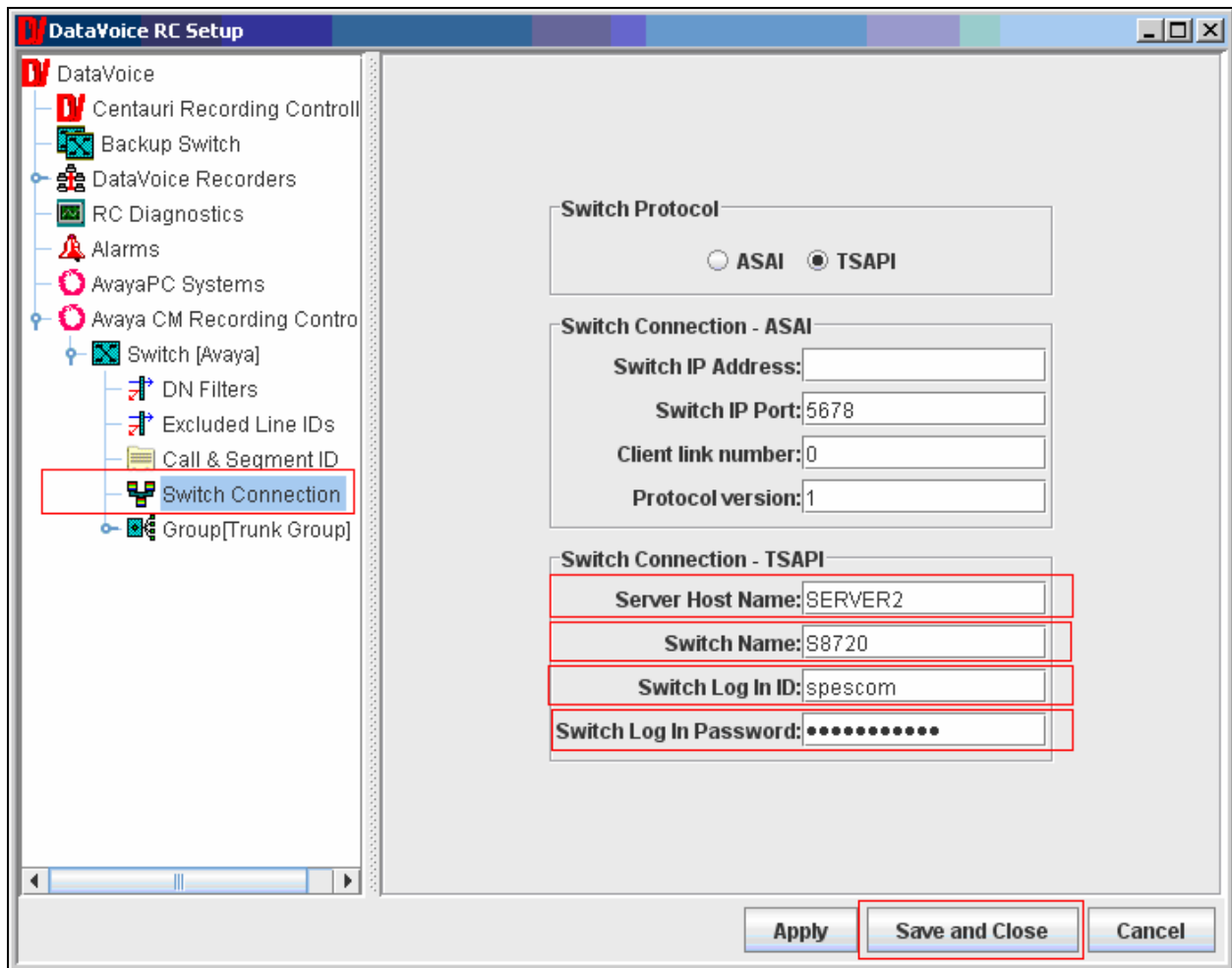
5.1.1. Configure TSAPI connection.

This section describes configuration steps for the connection to the Avaya Application Enablement Services (AES) server using the Telephony Services Application Programming Interface (TSAPI).

Navigate to the **DataVoice → Avaya CM Recording Controller → Switch [Avaya] → Switch Connection** page. Provide the following information under the Switch Connection – TSAPI section:

- Server Host Name
- Switch Name
- Switch Login ID
- Switch Login Password

After the completion, click on the **Save and Close** button.



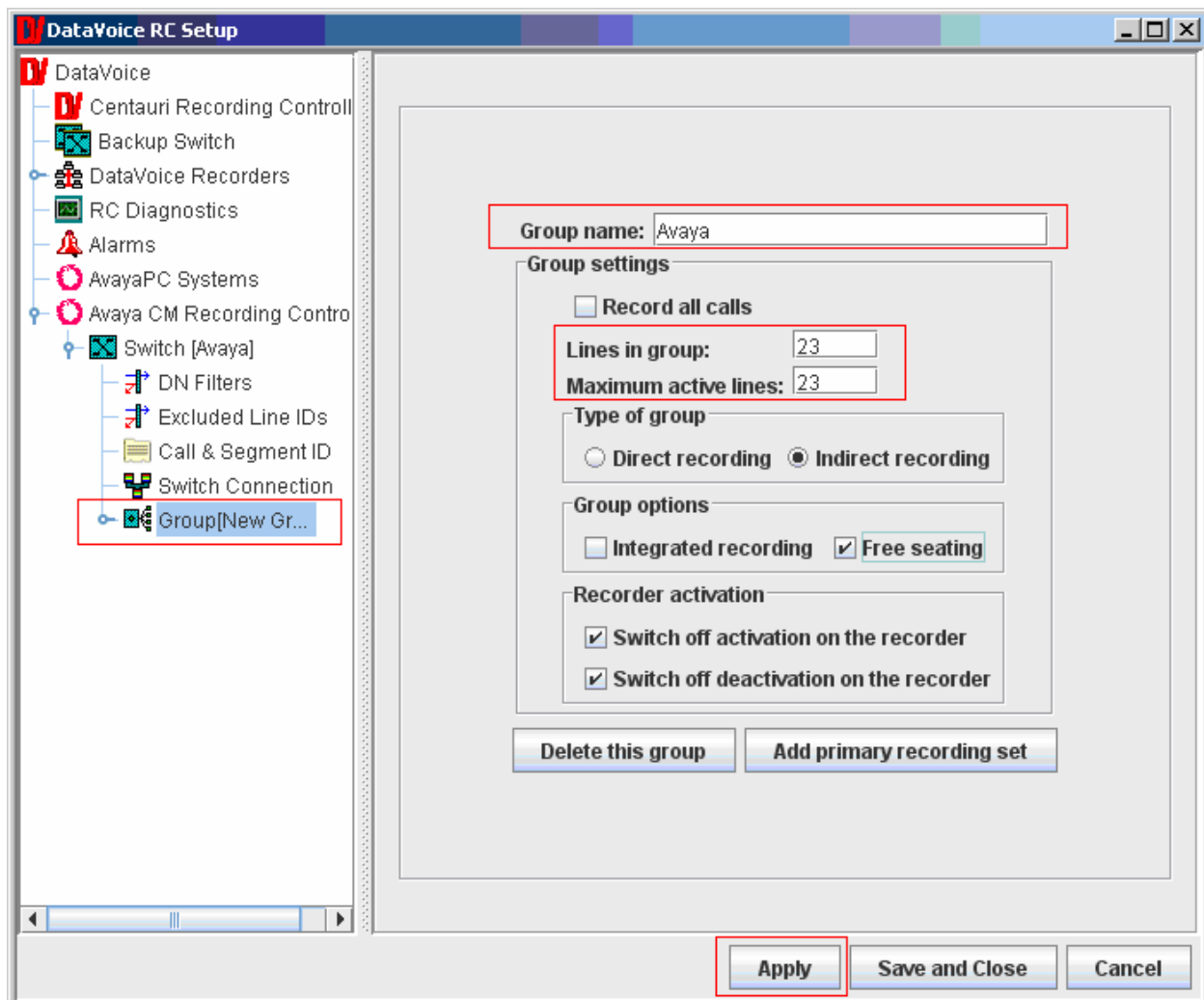
5.1.2. Configure Indirect Recording

This section describes configuration steps to setup indirect recording for the Recording Controller.

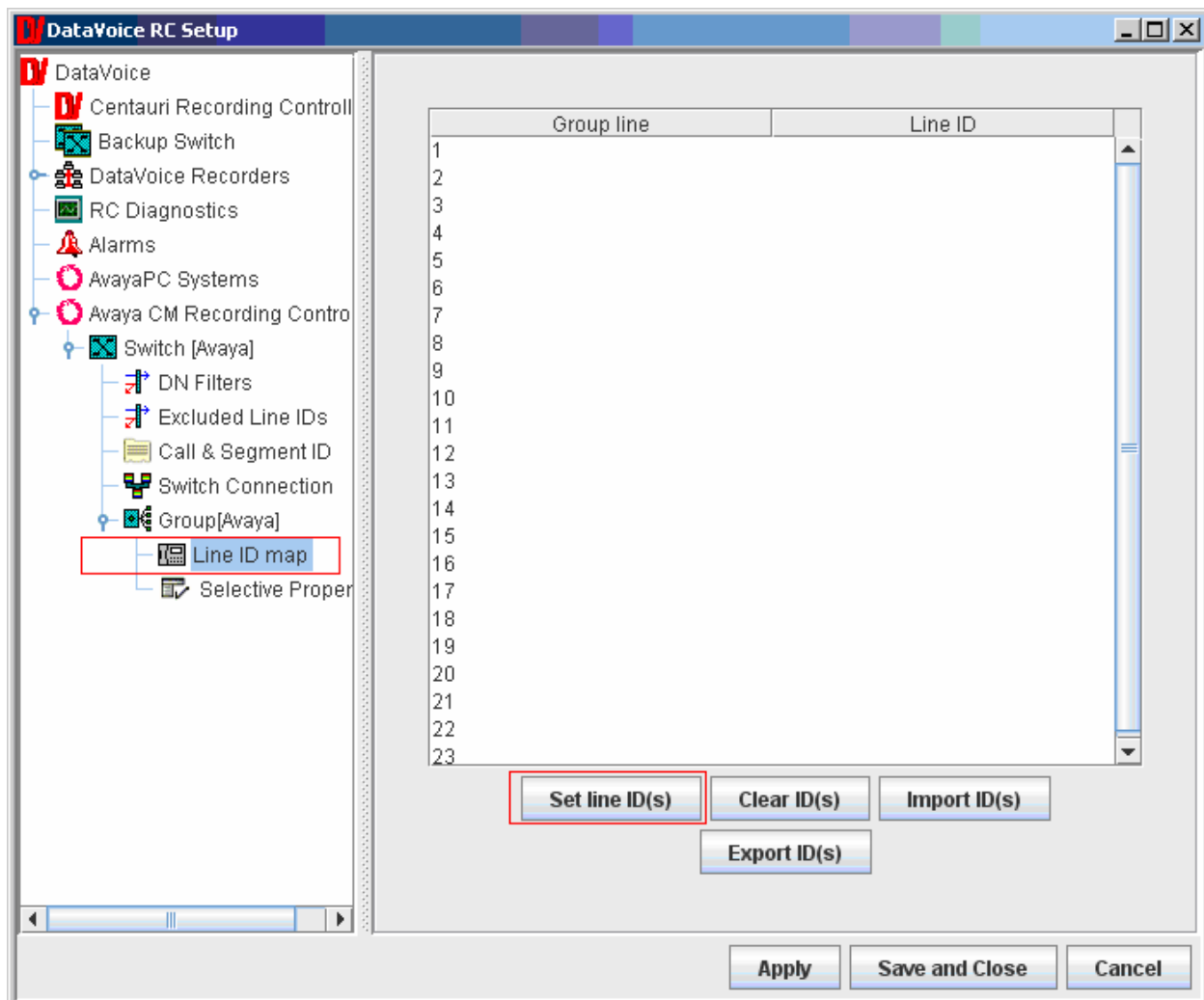
Navigate to **DataVoice → Avaya CM Recording Controller → Switch [Avaya] → Group[New Group]**. Provide the following information:

- Group Name – A descriptive name for the group
- Lines in group – Available lines for a trunk. For the compliance test, 23 trunk members were utilized for a T1 connection.
- Maximum active lines – The maximum number of active lines during the test were 23.

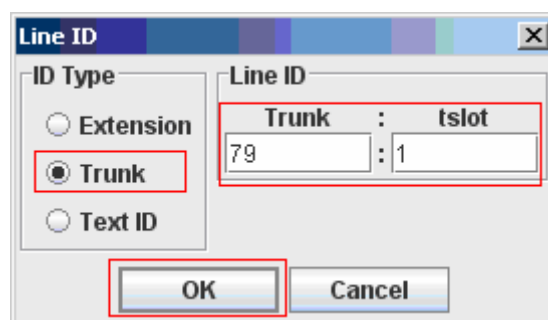
Default values may be used in the remaining fields. Click on the **Apply** button.



Navigate to **DataVoice** → **Avaya CM Recording Controller** → **Switch [Avaya]** → **Group[Avaya]** → **Line ID map**. Select **Set line ID(s)**.



From the Line ID window, select **Trunk** under ID type section. Provide the trunk group number that will be used. Type **1** for the tslot field. Click on the **OK** button.



5.1.3. Configure Integrated Recording

This section describes configuration steps to set up integrated recording for the Recording Controller.

Navigate to **DataVoice → Avaya CM Recording Controller → Switch [Avaya] → Group[New Group]**. Provide the following information:

- Group Name – A descriptive name for the group
- Lines in group – The lines in group were 30 during the test.
- Maximum active lines – The maximum number of active lines were 30 during the test.

Default values may be used in the remaining fields. Click on the **Apply** button.

The screenshot shows the 'DataVoice RC Setup' window. On the left is a tree view with the following structure:

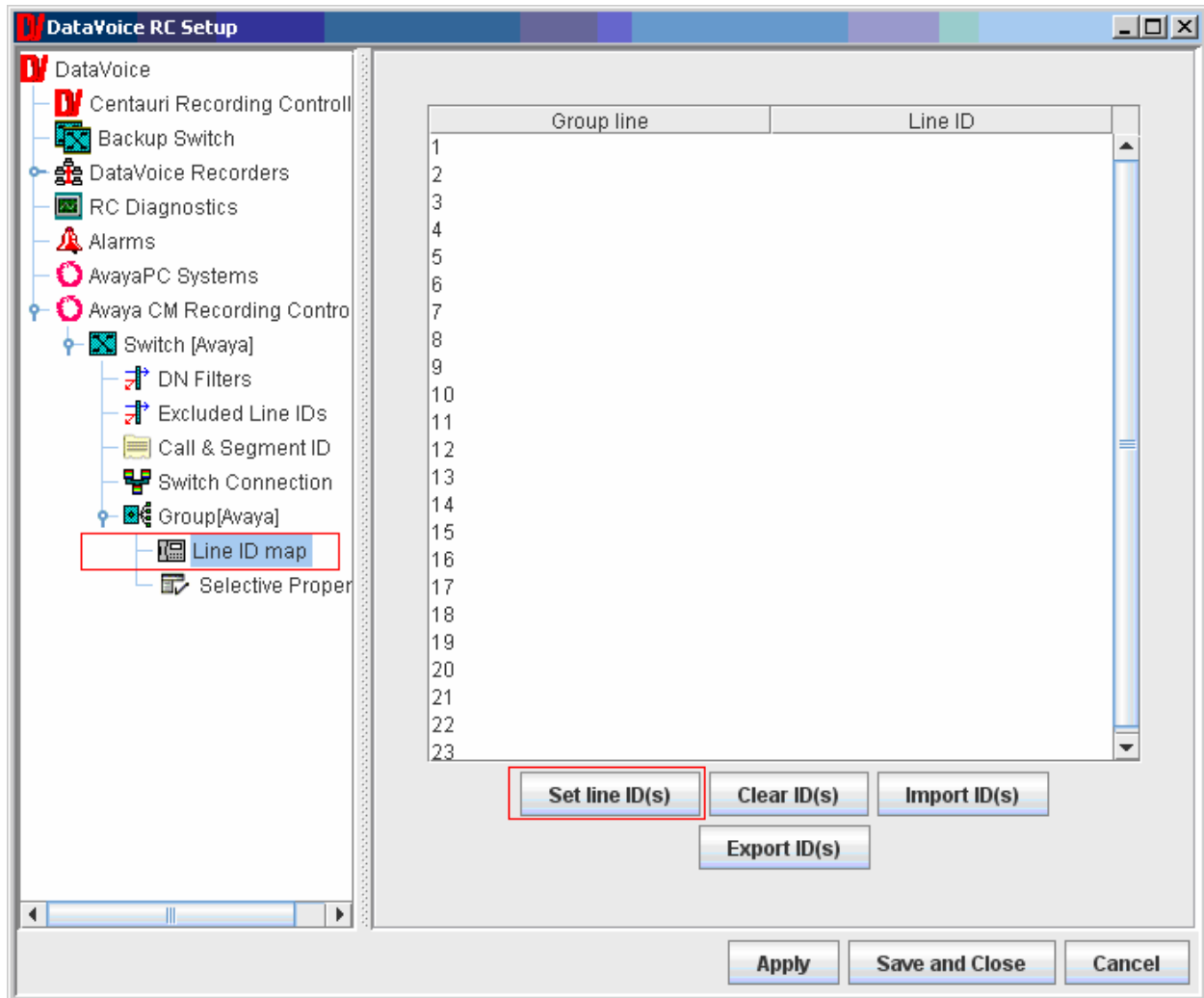
- DataVoice
 - Centauri Recording Controll
 - Backup Switch
 - DataVoice Recorders
 - RC Diagnostics
 - Alarms
 - AvayaPC Systems
 - Avaya CM Recording Contro
 - Switch [Avaya]
 - DN Filters
 - Excluded Line IDs
 - Call & Segment ID
 - Switch Connection
 - Group[New Gr...**

The 'Group[New Gr...' item is selected and highlighted with a red box. The main pane on the right displays the configuration for this group:

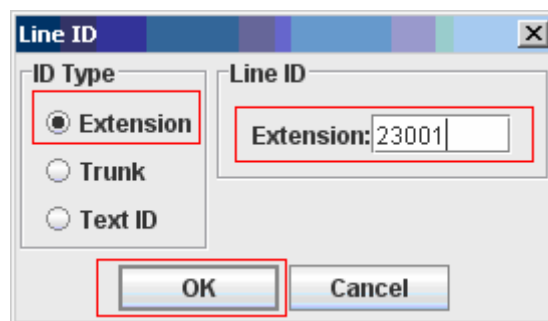
- Group name:** Avaya (text field, highlighted with a red box)
- Group settings**
 - ☐ Record all calls
 - Lines in group:** 30 (text field, highlighted with a red box)
 - Maximum active lines:** 30 (text field, highlighted with a red box)
 - Type of group**
 - ☐ Direct recording
 - ☐ Indirect recording
 - Group options**
 - ☒ Integrated recording
 - ☒ Free seating
 - Recorder activation**
 - ☒ Switch off activation on the recorder
 - ☒ Switch off deactivation on the recorder
- Buttons:** Delete this group, Add primary recording set

At the bottom of the window, the **Apply** button is highlighted with a red box, along with 'Save and Close' and 'Cancel' buttons.

Navigate to **DataVoice** → **Avaya CM Recording Controller** → **Switch [Avaya]** → **Group[Avaya]** → **Line ID map**. Select **Set line ID(s)**.



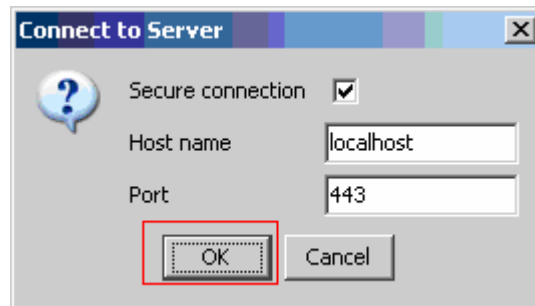
From the Line ID window, select **Extension** under ID type section. Provide the DMCC softphones that will be used. Click on the **OK** button.



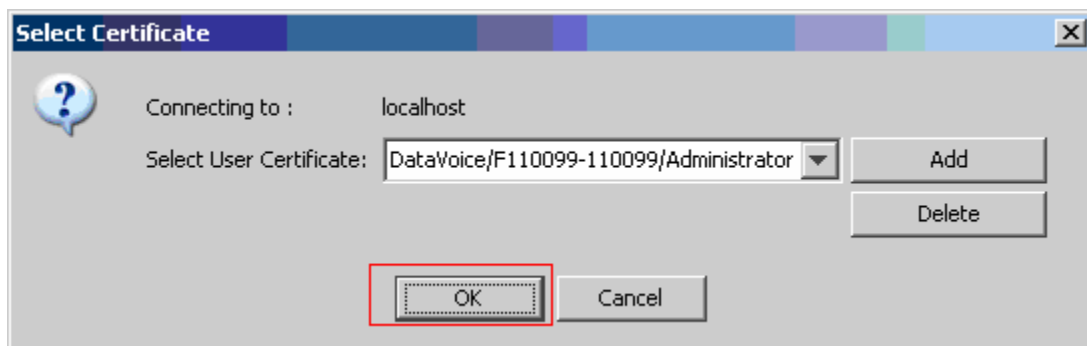
5.2. Configure DataVoice Libra Recorder

This section describes the setup of indirect and integrated recording for the Recorder.

The setup and configuration for the Recorder is done through the DataVoice AdminConsole. Open the AdminConsole by double-clicking the **AdminConsole** icon on the Windows Desktop. From the Connect to Server window, click on the **OK** button.



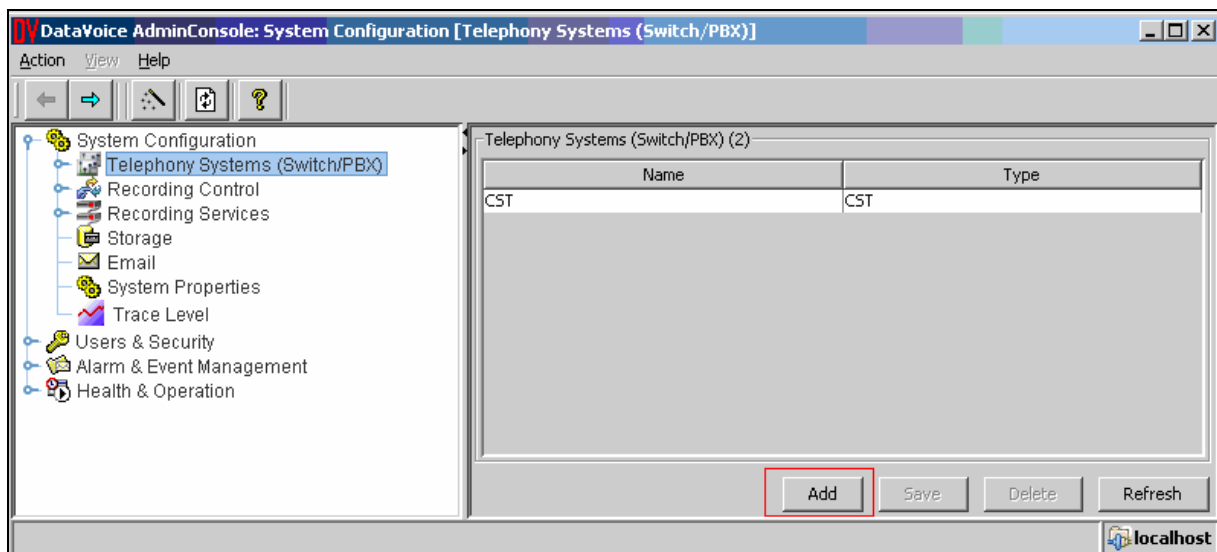
On the Select Certificate window, select **DataVoice/F110099/Administrator**, using the drop-down menu. This is the default selection. Click on the **OK** button.



5.2.1. Configure Indirect Recording

This section describes configuration steps to set up indirect recording on the Recorder.

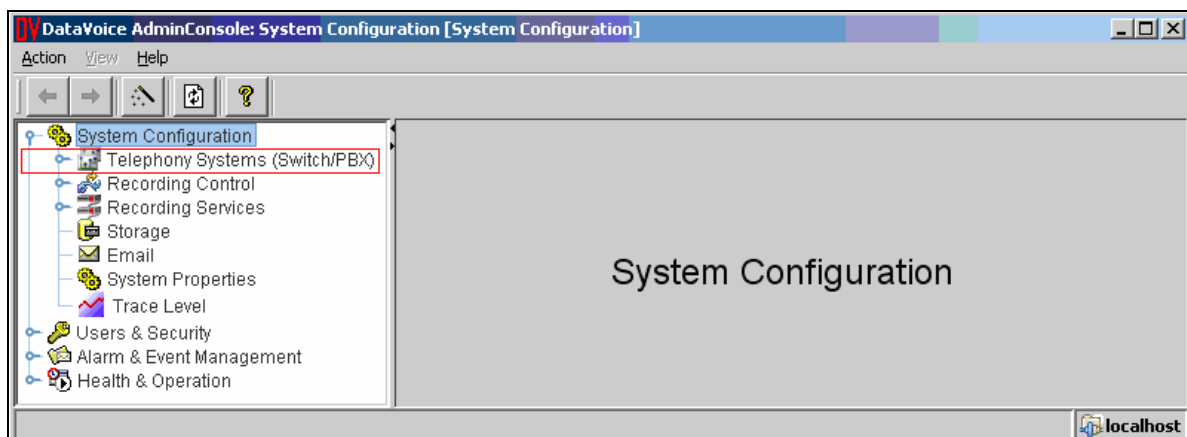
Libra uses the Ai-Logix SmartWORKS Digital Trunk card. When the Libra Recorder is installed all the setup and configuration is created automatically. Refer to [5] for a detailed overview of the setup and configuration.



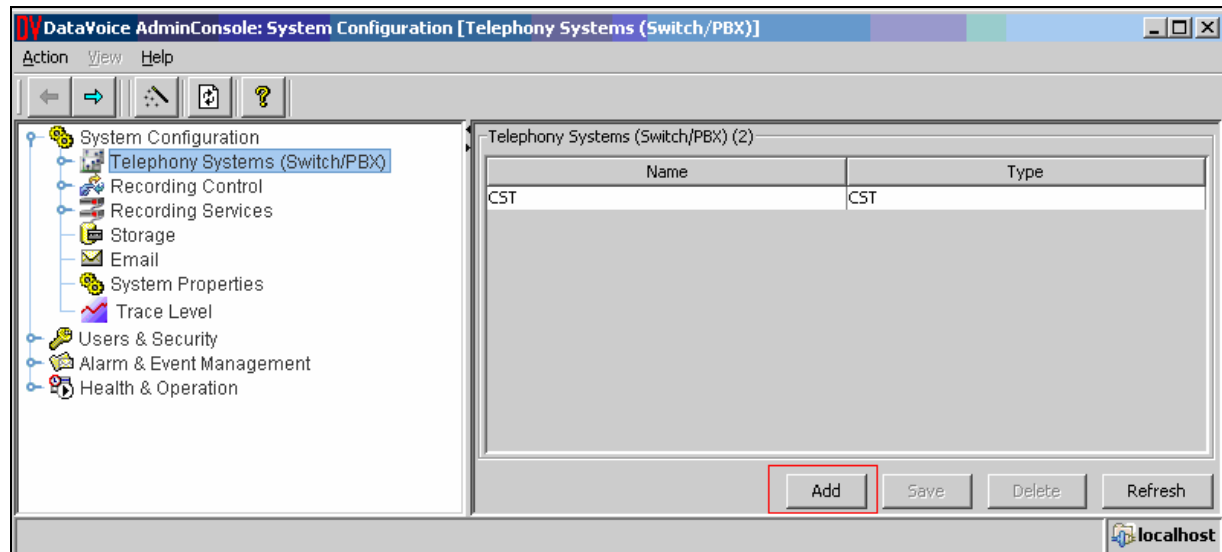
5.2.2. Configure Integrated Recording

This section describes configuration steps to set up integrated recording on the Recorder.

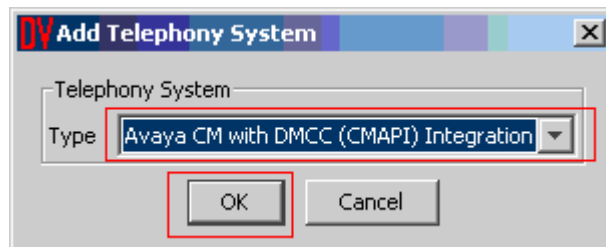
From the System Configuration page, select **System Configuration → Telephony Systems (Switch/PBX)**.



Click on the **Add** button to start configuring integrated recording.



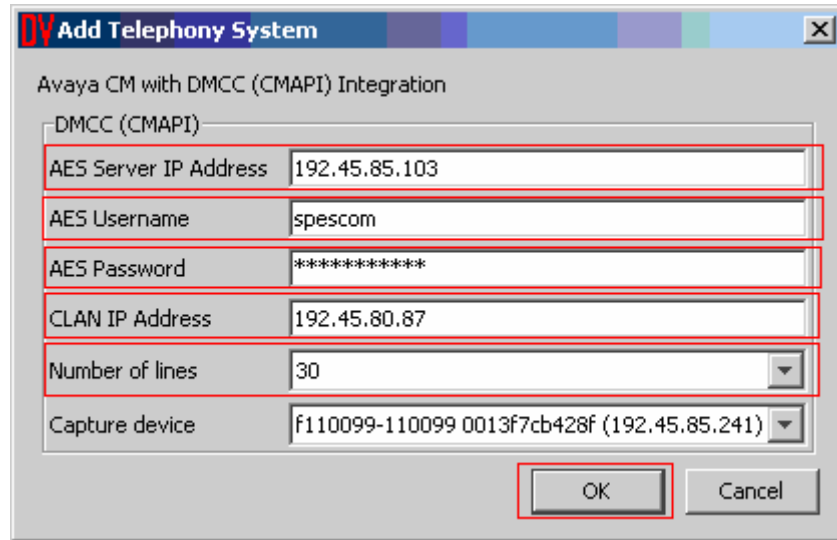
Select **Avaya CM with DMCC (CMAPI) Integration**, using the drop-down menu. Click on the **OK** button.



Provide the following information:

- AES Server IP Address – Enter the IP address of the AES server.
- AES Username – Enter the User Id created in **Section 4.3**.
- AES Password – Enter the User Password created in **Section 4.3**.
- CLAN IP Address – Enter the CLAN IP address that DMCC stations are registered to.
- Number of lines

Click on the **OK** button.



Add Telephony System

Avaya CM with DMCC (CMAPI) Integration

DMCC (CMAPI)

AES Server IP Address: 192.45.85.103

AES Username: spescom

AES Password: *****

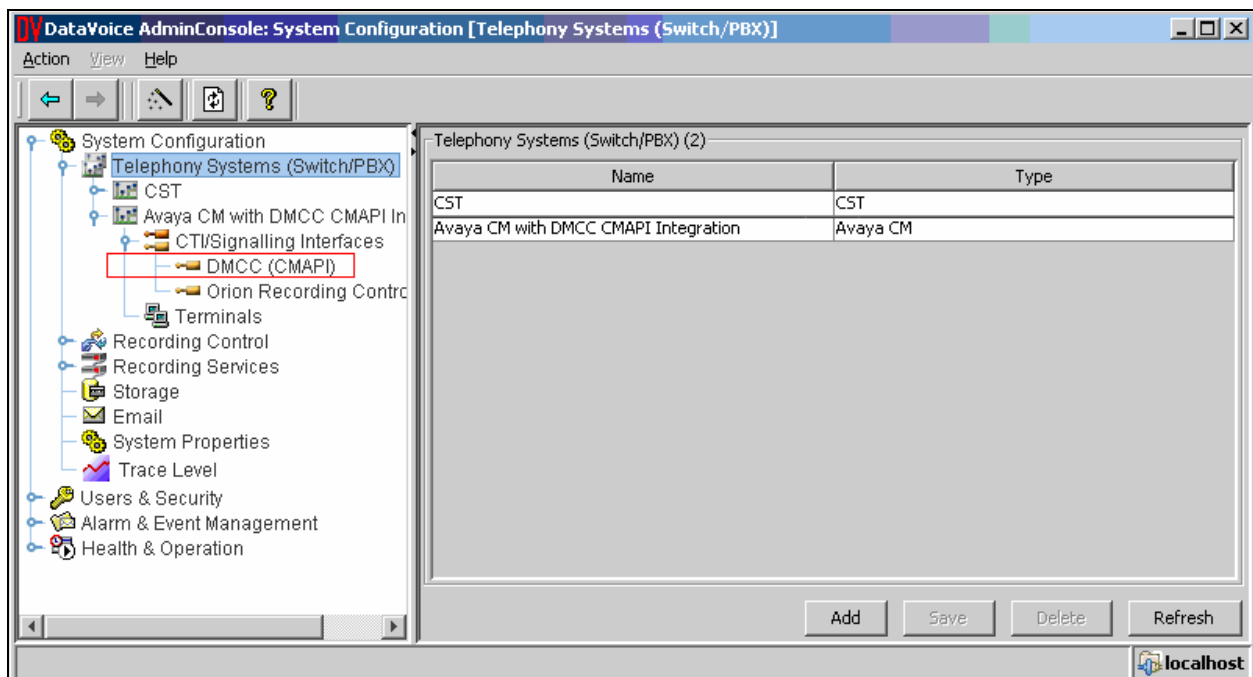
CLAN IP Address: 192.45.80.87

Number of lines: 30

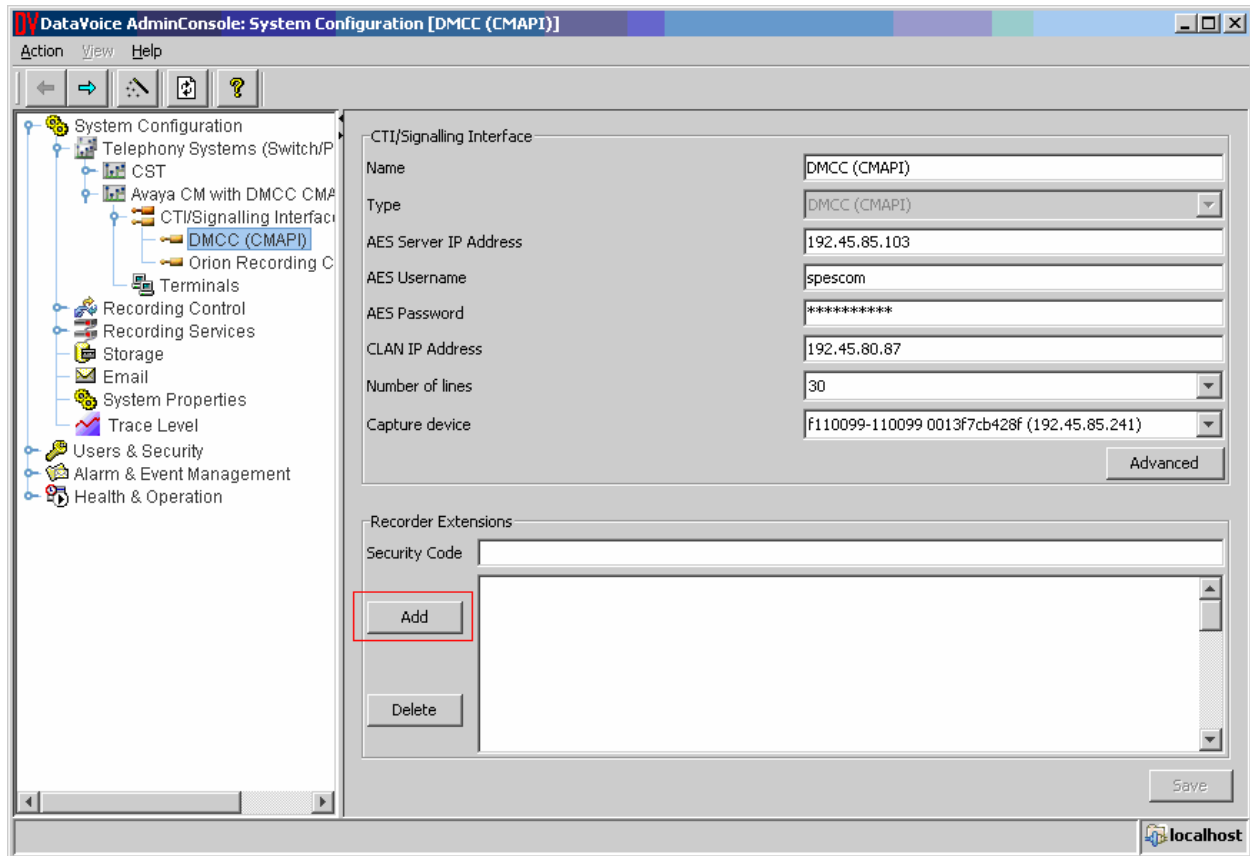
Capture device: f110099-110099 0013f7cb428f (192.45.85.241)

OK Cancel

After completion, the System Configuration window displays the new telephony system, called **Avaya CM with DMCC (CMAPI) Integration**. To add DMCC stations for recording, navigate to **System Configuration → Telephony Systems (Switch/PBX) → Avaya CM with DMCC CMAPI Integration → CTI Signalling Interfaces → DMCC (CMAPI)**.

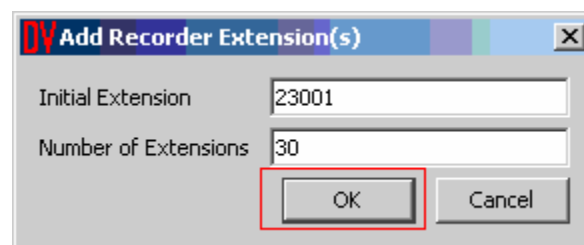


Click on the **Add** button under the Recorder Extensions section to configure the DMCC softphones.

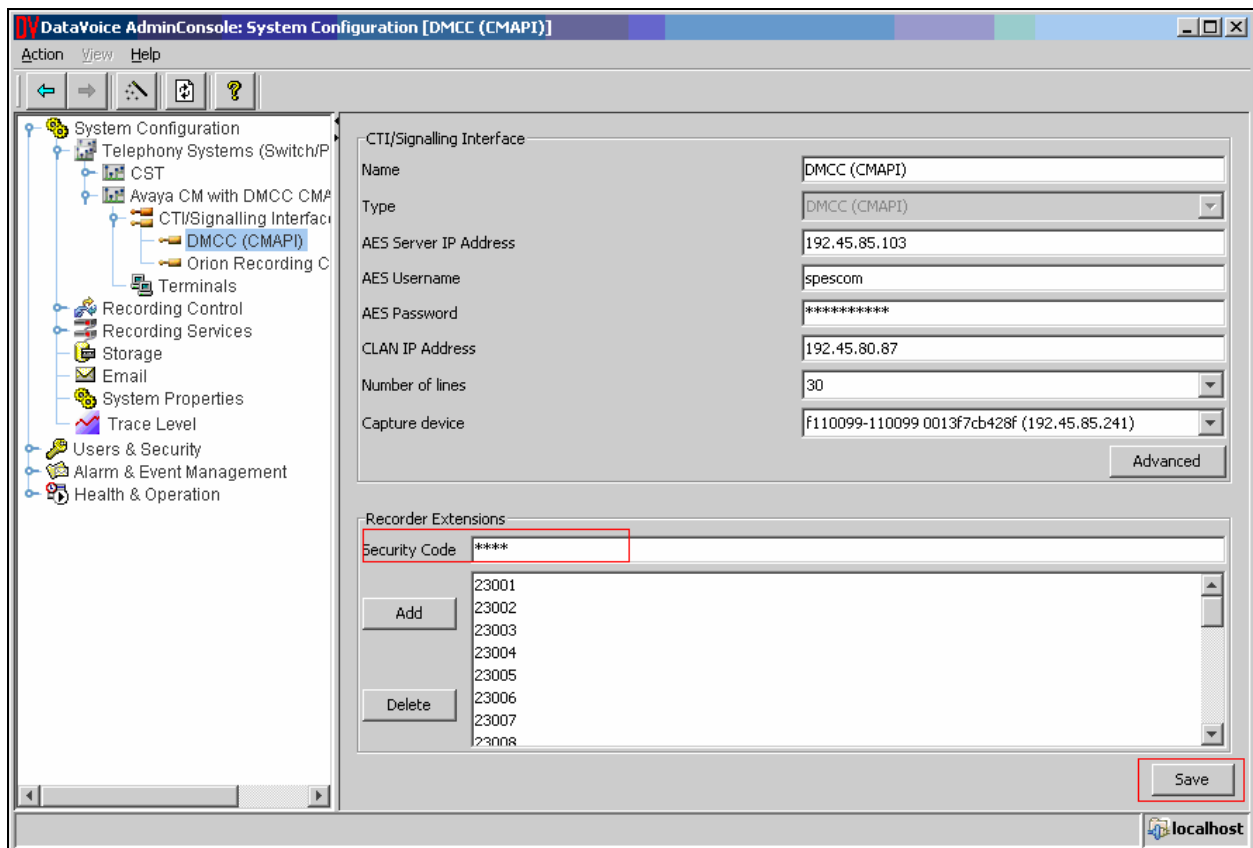


On the Add Recorder Extension(s) window, provide initial extension (softphone) and number of extensions (softphones).

Click the **OK** button.



After completion, provide the security code for the DMCC softphones.
Click on the **Save** button.



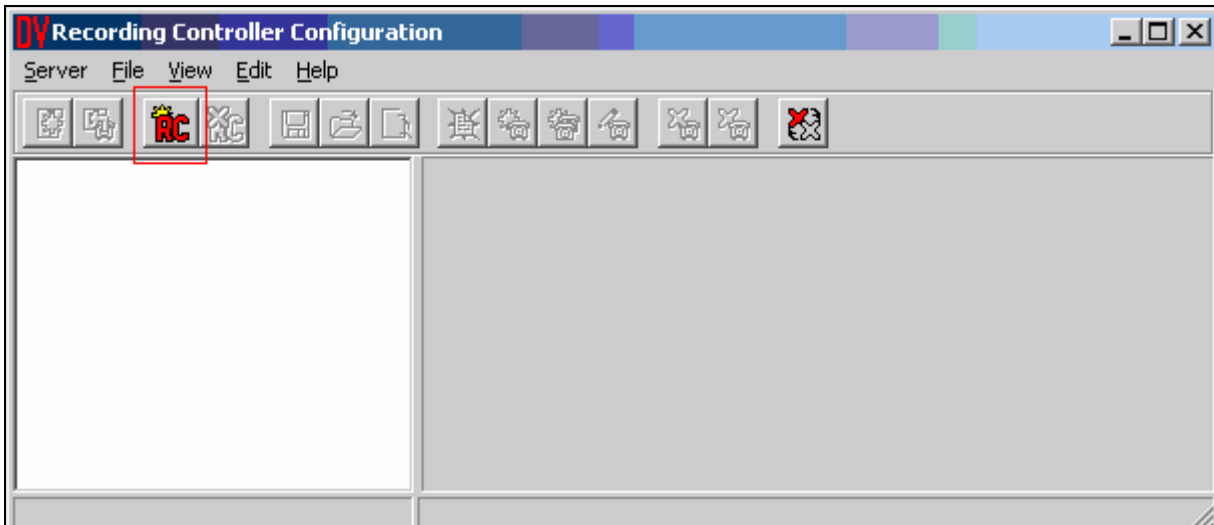
5.3. Configure Monitored Devices

This section describes the setup of the monitored devices for indirect and integrated recording.

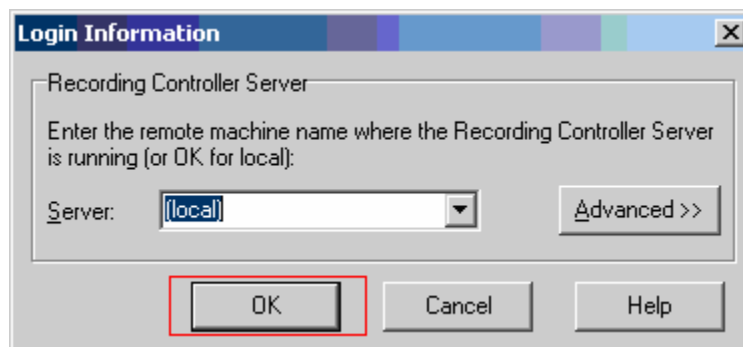
The dynamic configuration for the Recording Controller is done through the DataVoice Recording Controller Configuration Utility.

From the Windows desktop, navigate to **All Program → DataVoice → Definity RC → Recording Controller Configuration** to open the utility.

On the Recording Controller Configuration window, click the **RC** button to open a connection to the Recording Controller.

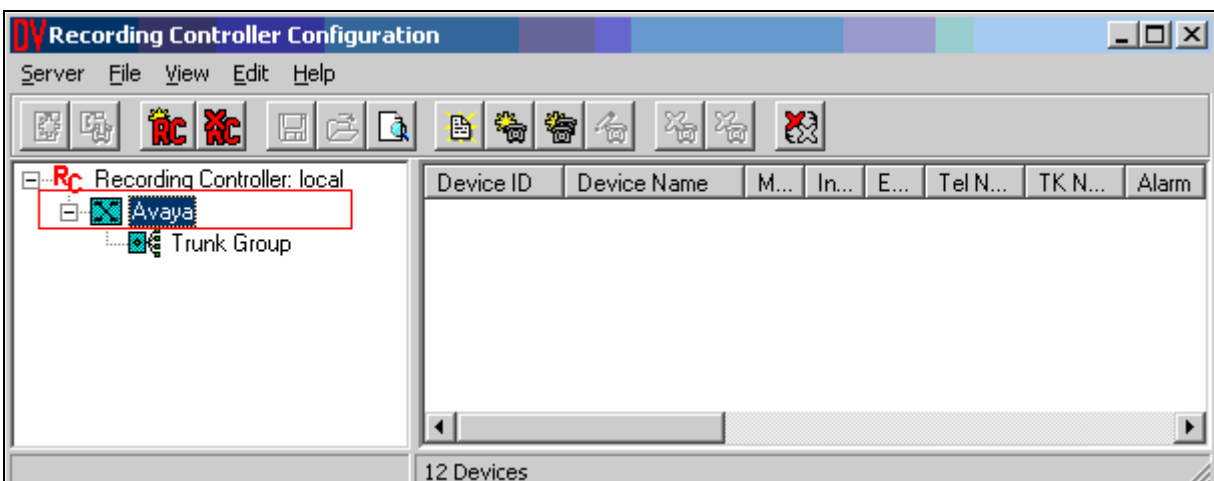


The following Login Information window appears. Click on the **OK** button.

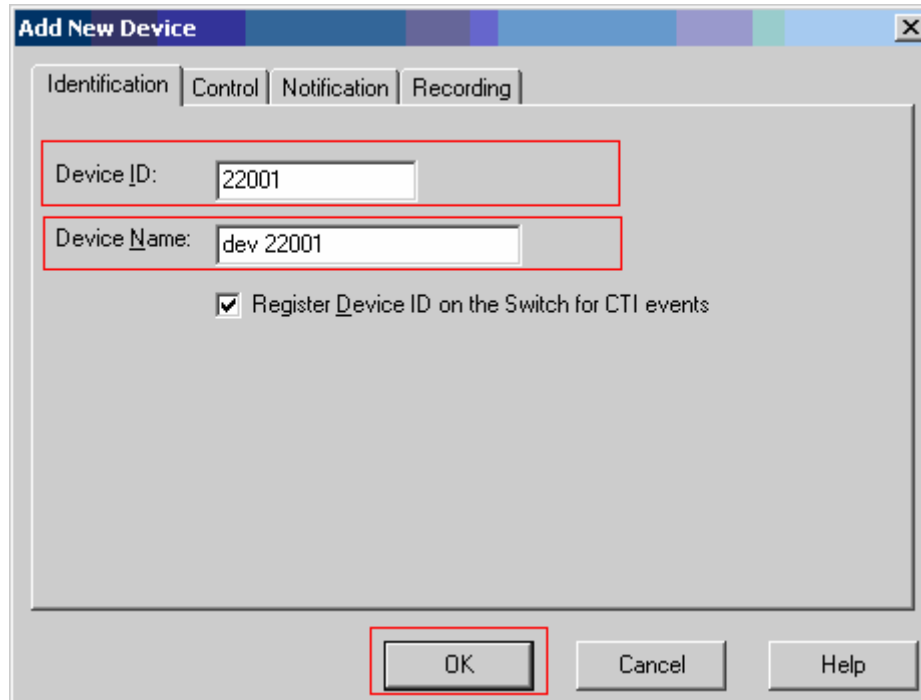


5.3.1. Configure Indirect Recording

This section describes configuration steps to set up monitored devices for indirect recording. Select **Avaya** under the RC Recording Controller:local section, from the left pane of the window. On the right pane of the window, click on the right mouse button, and select **Add New Device**.

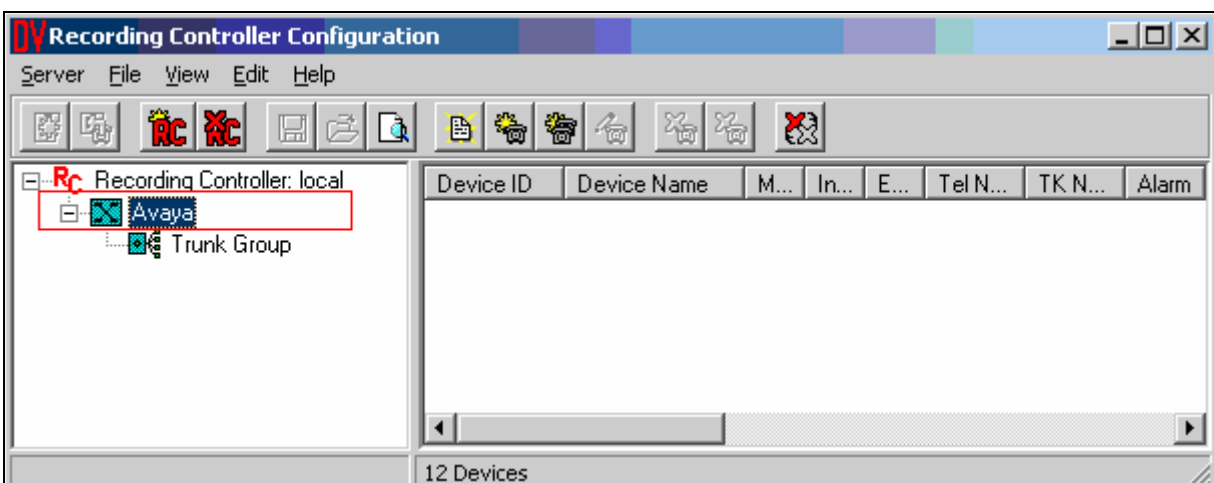


Provide **Device ID** and **Device Name** for each monitored device.
Click on the **OK** button.
Repeat this step to add all monitored devices.



The 'Add New Device' dialog box has a title bar with a close button. It contains four tabs: 'Identification', 'Control', 'Notification', and 'Recording'. The 'Identification' tab is active. It features two text input fields: 'Device ID:' with the value '22001' and 'Device Name:' with the value 'dev 22001'. Both fields are highlighted with red rectangles. Below these fields is a checkbox labeled 'Register Device ID on the Switch for CTI events' which is checked. At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'. The 'OK' button is highlighted with a red rectangle.

Another way to add multiple monitored devices is by utilizing the range of device button. From the Recording Controller Configuration window, select **Avaya** under the RC Recording Controller:local section, from the left pane of the window. On the right pane of the window, click on the right mouse button, and select **Add New Range of Devices**.



Provide **Device ID From** and **To** and descriptive name for the Device Name field.
Click on the **OK** button.

The screenshot shows a Windows-style dialog box titled "Add New Range of Devices". It has four tabs: "Identification", "Control", "Notification", and "Recording". The "Identification" tab is active. Inside the dialog, there are three input fields: "Device ID From:" with the value "22002", "To:" with the value "22002", and "Device Name:" with the value "dev 22001". Below these fields is a checked checkbox labeled "Register Device ID on the Switch for CTI events". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help". The "OK" button is highlighted with a red rectangular box.

5.3.2. Configure Integrated Recording

Repeat all steps described in section 5.3.1 to add monitored devices for integrated recording.

6. Interoperability Compliance Testing

The interoperability compliance test included basic recording, serviceability, and performance testing. The basic recording testing evaluated the ability of the DataVoice Recording Solution for Avaya Communication Manager to monitor and record calls placed to and from stations. The serviceability testing introduced failure scenarios to see if the DataVoice Recording Solution for Avaya Communication Manager can resume recording after failure recovery. The performance testing stressed the DataVoice Recording Solution for Avaya Communication Manager by continuously placing calls over extended periods of time.

6.1. General Test Approach

The general approach was to manually place calls to and from stations, monitor and record them using the DataVoice Recording Solution for Avaya Communication Manager, and verify the recordings. The types of calls included internal calls, inbound and outbound trunk calls. Performance tests verified that the DataVoice Recording Solution for Avaya Communication Manager could record calls during a sustained, high volume of calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, and resets were applied.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

This section provides the steps that can be performed to verify proper configuration of Avaya Communication Manager and Avaya AES.

7.1. Verify Avaya Communication Manager

Verify the status of the administered AES link by using the **status aesvcs link** command.

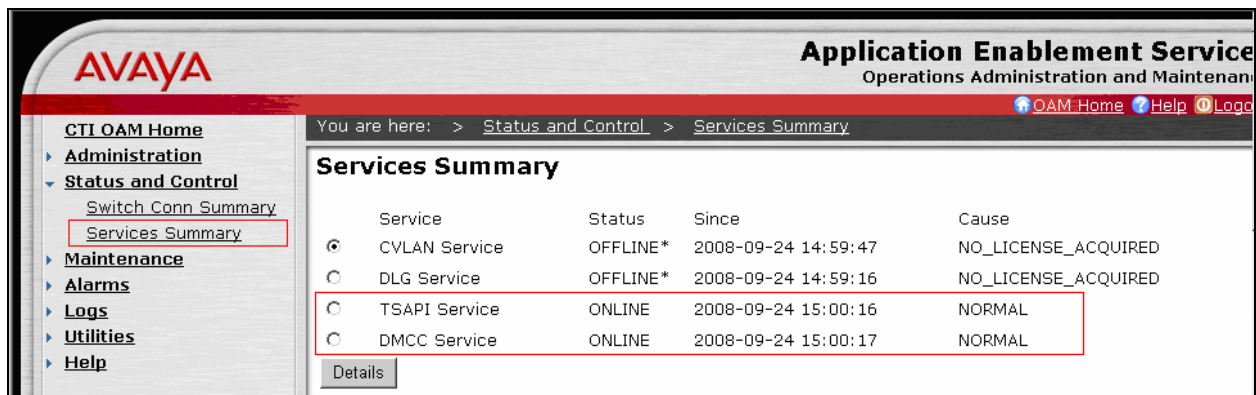
status aesvcs link						
AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	server2	192. 45. 80.103	60336	CLAN-AES	208	197

Verify the Service State field of the administered TSAPI CTI link is in **established** state, by using the **status aesvcs cti-link** command.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
4	4	no	server2	established	15	15

7.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services are ONLINE, by selecting **Status and Control** → **Services Summary** from the left pane.



AVAYA Application Enablement Service
Operations Administration and Maintenance

You are here: > [Status and Control](#) > [Services Summary](#)

Services Summary

Service	Status	Since	Cause
<input checked="" type="radio"/> CVLAN Service	OFFLINE*	2008-09-24 14:59:47	NO_LICENSE_ACQUIRED
<input type="radio"/> DLG Service	OFFLINE*	2008-09-24 14:59:16	NO_LICENSE_ACQUIRED
<input type="radio"/> TSAPI Service	ONLINE	2008-09-24 15:00:16	NORMAL
<input type="radio"/> DMCC Service	ONLINE	2008-09-24 15:00:17	NORMAL

[Details](#)

8. Support

Technical support on the DataVoice Recording Solution can be obtained via email at www.datavoice.spescom.com or by calling 27-11-266-1801.

9. Conclusion

These Application Notes illustrate the procedures for configuring the DataVoice Recording Solution to monitor and record calls placed to and from stations on an Avaya Communication Manager system. In the integrated recording configuration described in these Application Notes, the DataVoice Recording Solution employs DMCC virtual stations as recording ports. The recording formats tested were SSC (for integrated recording) and trunk tap. During compliance testing, the DataVoice Recording Solution successfully monitored events and recorded calls placed to and from stations. The DataVoice Recording Solution was also able to record calls under continuous call volumes over extended periods of time.

10. Additional References

This section references the Avaya and DataVoice documentation that are relevant to these Application Notes.

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

[1] *Administrator Guide for Avaya Communication Manager*, Issue 4, January 2008, Document Number 03-300509

[2] *Application Enablement Services Administration and Maintenance Guide*, Release 4.1, Issue 9, February 2008, Document Number 02-300357

The following documentation was provided by Spescom DataVoice

[3] *RCL-RC0-HBT-13 RC Server cV10.9 Tech Manual v1.3*

[4] *RCL-DEF-HBT-07 Avaya CM PI cV3.6 Technical Manual v1.4*

[5] *LIB-GEN-HBT-01 Libra and Nexus Technical Manual v2.8*

©2008 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.