



Avaya Solution & Interoperability Test Lab

Configuring NICE Call Recording System – CLS and VoIP Logger with Avaya Application Enablement Services Release and Avaya Communication Manager – Issue 1.0

Abstract

These Application Notes describe how to configure the NICE Call Recording System with the Avaya Application Enablement Services and Avaya Communication Manager to record incoming and outgoing phone calls. The configuration described in these Application Notes focuses on the NICE Call Recording system designed for Public Safety Answering Point call takers.

Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab at the request of the Solutions Marketing Team.

TABLE OF CONTENTS

1.	Introduction.....	3
1.1.	Public Safety Solution Overview.....	3
1.2.	NICE Call Flows.....	4
1.3.	Interoperability Compliance Testing	4
1.4.	Support.....	4
2.	Configuration	5
2.1.	Public Safety Solution Reference Configuration.....	5
2.2.	Network Configuration	6
3.	Equipment and Software Validated	7
4.	Configure Avaya Communication Manager.....	7
4.1.	Verify Avaya Communication Manager License	8
4.2.	Administer IP Node Name for C-LAN.....	9
4.3.	Administer IP Interface for C-LAN.....	10
4.4.	Administer Data Module for C-LAN.....	11
4.5.	Administer IP Services for AES Transport Link	11
4.6.	Administer CTI Link for TSAPI Service.....	12
4.7.	Administer Stations for NICE.....	12
4.8.	Administer COR for Virtual and Monitored Stations.....	14
4.9.	Administer Feature Access code for Service Observing	15
4.10.	Administer System Parameters	15
5.	Configure Avaya Application Enablement Services	17
5.1.	Verify Avaya Application Enablement Services License.....	17
5.2.	Administer Local IP.....	19
5.3.	Administer Switch Connection	19
5.4.	Administer TSAPI Link.....	21
5.5.	Administer Security Database.....	22
5.6.	Obtain Tlink Name	24
5.7.	Administer NICE Users	24
5.8.	Administer Device Groups	26
5.9.	Restart TSAPI Service	29
6.	Configure NICE Call Recording System.....	30
6.1.	Configure NiceCLS server.....	30
6.2.	Configure the NICE Application Tools	41
7.	General Test Approach and Test Results.....	46
8.	Verification	46
8.1.	Verify Avaya Communication Manager.....	46
8.2.	Verify Avaya Application Enablement Services	47
8.3.	Verify Call Recording and Playback from the NICE Query and Monitor	49
9.	Terminology.....	50
10.	Conclusion	50
11.	Additional References.....	50

1. Introduction

These Application Notes describe how to configure the NICE Call Recording System with the Avaya Application Enablement Services (AES) and Avaya Communication Manager to record incoming and outgoing phone calls. The configuration described in these Application Notes focuses on the NICE Call Recording system designed for Public Safety Answering Point call takers.

NICE Call Recording System for Public Safety is comprised of NICE CLS 8.90.4 and VoIP Logger 9.10.05. The integration with Avaya Communication Manager is achieved through the Application Enablement Services – Telephony Services Application Programming Interface (TSAPI) & Device, Media and Call Control Interface (DMCC) services.

The NICE CLS uses Avaya AES to register IP Softphones and receive call status and call events from Avaya Communication Manager. The VoIP Logger creates recording channels which emulate IP Softphones to receive audio streams. The NICE CLS Server manages an SQL database including extensive call details. Using NICE application tools, recorded calls with call detail information can be queried and played back.

For the Public Safety solution, NICE Call Recording application is achieved through the Avaya Communication Manager service observing feature. This option is selected at the installation phase in NICE application. (Note: NICE recording features can be enabled or disabled during the software installation only). This option allows automatic recording of entire calls for all configured stations. NICE application uses TSAPI of Avaya AES to observe and record the calls. This mode uses DMCC controlled IP softphones that are automatically allocated in NICE as shared ports for call recording.

1.1. Public Safety Solution Overview

The Avaya Public Safety Solution is designed to help government and private agencies responsible for the delivery of public safety services to enterprises and civilian populations. This includes:

- ✦ **Avaya Contact Center** applications such as expert agent selection to ensure the most qualified and most available resource rapidly attends to the case.
- ✦ **PlantCML Sentinel CM and Intelligent Work Station** integration which provides the public safety community with call-center solutions designed to streamline emergency call-taking. Sentinel CM is a 911 incident management solution, and integration with Avaya Communication Manager is achieved through the Avaya Application Enablement Services (AES) Telephony Services Application Programming Interface (TSAPI) & Device, Media and Call Control Interface (DMCC) services.
- ✦ **Raytheon JPS ACU-2000IP Intelligent Interconnect System** integration which provides seamless communication across traditionally disparate communications such as Land-based Mobile Radio (LMR). The ACU-2000IP is a radio IP/SIP gateway that

allows IP-PBX stations to interface with radios. Multiple interface cards allow all radios to be a part of the IP-PBX system. Integration with Avaya Communication Manager is achieved through the SIP Enablement Services (SES).

- ↳ **NICE CLS/VoIP Logger** integration for secure recording of audio on the entire chain of service delivery from the conversations with the citizen, to command and control and dispatch, to resolution.

1.2. NICE Call Flows

1. NICE CLS connects to the AES DMCC services and requests to initiate the emulation of IP Softphones, registering one phone per recording channel.
2. NICE CLS receives a Start call event from the AES.
3. Based on the user defined recording rules, NICE CLS determines whether the call needs to be recorded. If so, NICE CLS allocates an IP address and port for recording on the VoIP Logger and sends a request, to Avaya Communication Manager via the AES to observe the call.
4. Avaya Communication Manager sends audio RTP streams to the NICE VoIP Logger and it records the audio in the allocated recording channel.
5. When the call ends, NICE CLS requests to stop recording the call.

1.3. Interoperability Compliance Testing

Interoperability compliance testing focused on NICE Call Recording System's ability to work with Avaya Application Enablement Services Release 4.2.1 and Avaya Communication Manager Release 5. Call recording and playback was verified for incoming/outgoing calls. In addition, phone features like hold, conference calls and transfers were exercised while the call is being recorded. The call recording functionality was verified for incoming and outgoing trunk calls, IP, SIP, Analog and DCP stations.

1.4. Support

Technical support on NICE can be obtained at www.nice.com.

2. Configuration

2.1. Public Safety Solution Reference Configuration

The reference configurations for Public Safety Solution are shown below in **Figure 1**.

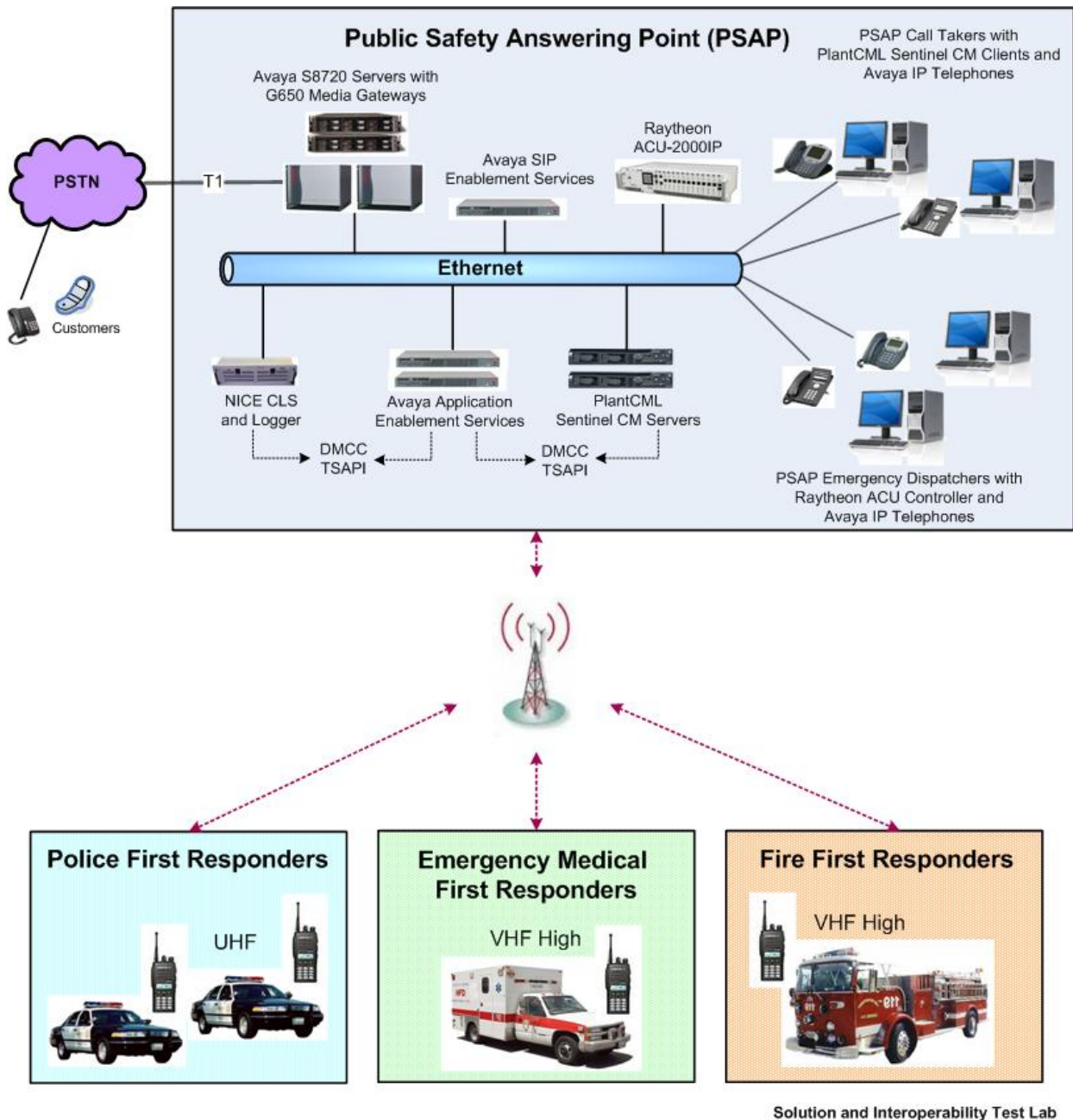


Figure 1: Avaya Public Safety Solution Reference Configuration

2.2. Network Configuration

The network implemented for the reference configuration is shown in **Figure 2**. The Public Safety Answering Point location consists of Avaya S8720 Servers controlling G650 Media Gateways. The PSAP location is also equipped with a pair of Avaya Application Enablement Services (AES) servers, Avaya IP phones, a pair of PlantCML Sentinel CM servers and multiple Sentinel 9-1-1 clients. Please refer to [4] for PlantCML Sentinel CM configuration details.

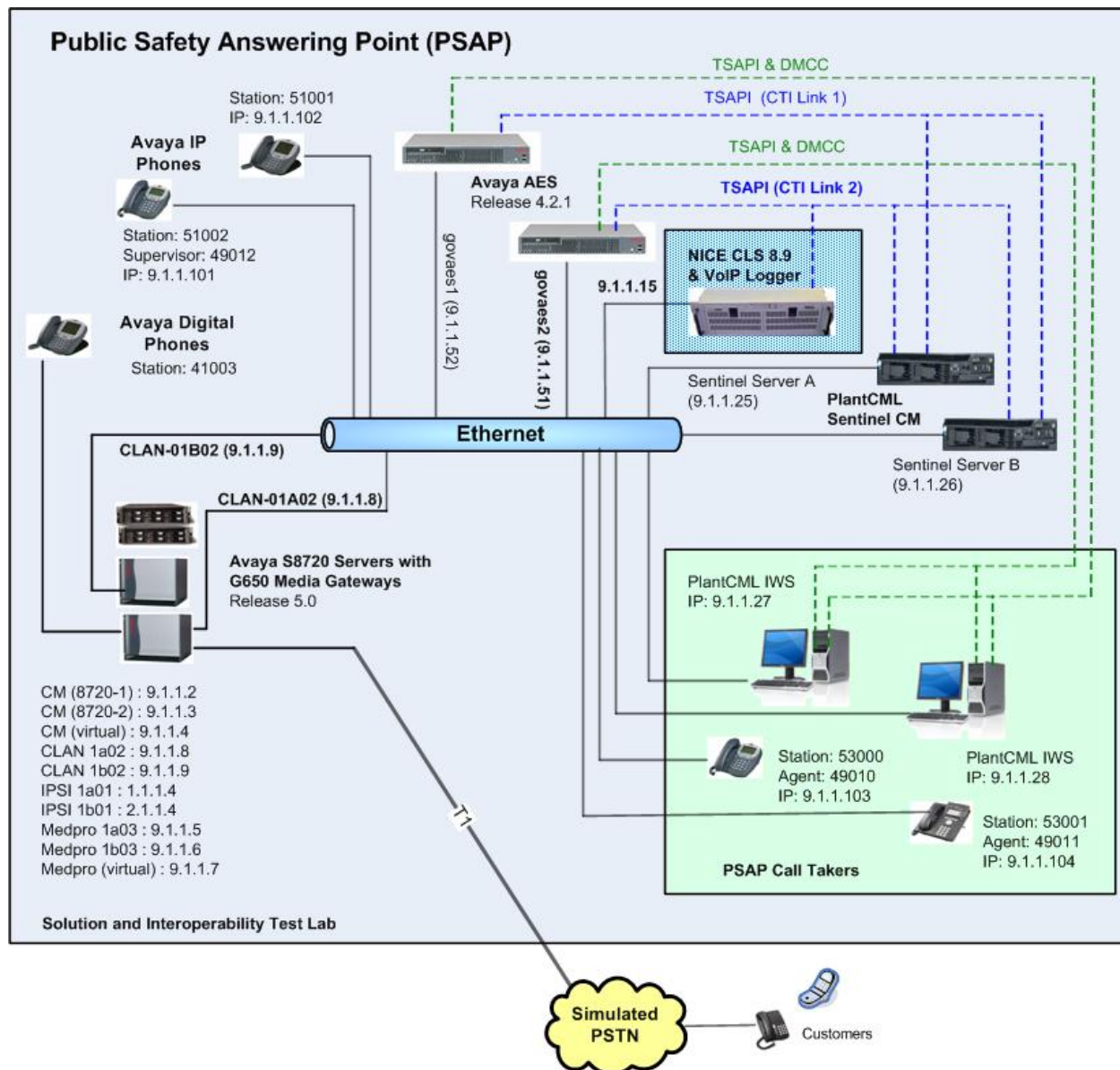


Figure 2: Network Configuration Diagram

3. Equipment and Software Validated

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

Device Description	Versions Tested
Avaya Communication Manager - S8720 Servers	Release 5.0 (R015x.00.0.825.4)
Avaya G650 Media Gateway - IPSI (TN2312BP) - CLAN (TN799DP) - MedPro (TN2602AP)	- HW15 FW044 - HW01 FW026 - HW02 FW044
Avaya AES	Release 4.2.1 (Build 20-5)
Avaya 4600 Series H.323 Telephones	R2.8
Avaya 9600 Series H.323 Telephones	R1.5
Avaya IP Softphone	R6.0
Avaya 6211 Analog Telephones	N/A
Avaya 2420 Digital Telephones	N/A
PlantCML Sentinel - Sentinel CM Server - Sentinel Intelligent Workstation	Release 2 (Build 7) OS for the IWS is Windows XP Professional SP 2
NICE Call Recording - CLS - VoIP Logger	8.90.4 9.10.05

4. Configure Avaya Communication Manager

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

- Verify Avaya Communication Manager License
- Administer IP node name for C-LAN
- Administer IP interface for C-LAN
- Administer data module for C-LAN
- Administer IP services for AES transport link
- Administer CTI link for TSAPI service
- Administer stations for NICE
- Administer system parameters
- Administer feature access codes

4.1. Verify Avaya Communication Manager License

Log into the System Access Terminal (SAT) to verify that Avaya 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 **ASAI Link Core Capabilities**, and **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? n	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	Backup Cluster Automatic Takeover? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Branch? n	
Answer Supervision by Call Classifier? y	CAS Main? n	
ARS? y	Change COR by FAC? n	
ARS/AAR Partitioning? y	Computer Telephony Adjunct Links? y	
ARS/AAR Dialing without FAC? y	Cvg Of Calls Redirected Off-net? y	
ASAI Link Core Capabilities? y	DCS (Basic)? y	
ASAI Link Plus Capabilities? y	DCS Call Coverage? Y	

Navigate to **Page 6**, and verify that the **Service Observing (Basic)** and **Service Observing (Remote/by FAC)** are set to “y”. NICE Call Recording applications will use the Avaya Communication Manager feature Service Observing with Multiple Observers. Multiple observers on the same call is not supported for Service Observing by VDN feature.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 5.0		
ACD? y	Reason Codes? y	
BCMS (Basic)? y	Service Level Maximizer? n	
BCMS/VuStats Service Level? y	Service Observing (Basic)? y	
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y	
Business Advocate? y	Service Observing (VDNs)? y	
Call Work Codes? y	Timed ACW? y	
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y	
Dynamic Advocate? y	Vectoring (Prompting)? y	
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? Y	

Navigate to **Page 10**, and verify that there are sufficient **IP_API_A** licenses.

display system-parameters customer-options		Page 10 of 11
MAXIMUM IP REGISTRATIONS BY PRODUCT ID		
Product ID	Rel. Limit	Used
IP_API_A	: 100	4
IP_API_B	: 100	0
IP_API_C	: 100	0
IP_Agent	: 300	0
IP_IR_A	: 0	0
IP_Phone	: 12000	5
IP_ROMax	: 12000	0
IP_Soft	: 300	0
IP_eCons	: 0	0

4.2. Administer IP Node Name for C-LAN

Enter the “change node-names ip” command, and add an entry for the C-LAN that will be used for connectivity to the AES server. For the sample configuration, use the following in the **Name** and **IP Address**. The actual node name and IP address may vary. Submit these changes.

C-LAN	
Name	IP Address
CLAN-01A02	9.1.1.8
CLAN-01B02	9.1.1.9

```
change node-names ip                                     Page 1 of 2
                                     IP NODE NAMES
      Name      IP Address
AES1            9.1.1.50
CLAN-01A02      9.1.1.8
CLAN-01B02      9.1.1.9
CLAN-RETAIL     30.1.1.4
FCSWinsuite     9.1.1.203
GVT-S8300-LSP   9.1.4.2
MedPro-01A03    9.1.1.5
MedPro-01B07    9.1.1.6
RedSky1         9.1.1.55
RedSky2         9.1.1.56
S8500-ESS       9.1.1.13
SES1            9.1.1.34
VAL-01A12       9.1.1.12
clan-trade      5.1.1.4
default         0.0.0.0
govmas1         9.1.1.31
( 16 of 17   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

4.3. Administer IP Interface for C-LAN

Add the C-LAN to the system configuration using the “add ip-interface <board location>” command. In the sample configuration, “1a02” for CLAN-01A02 and “1b02” for CLAN-01B02” will be used. Note that the actual slot number may vary. Enter the C-LAN node name assigned from **Section 4.2** into the **Node Name** field. The **IP Address** field will be populated automatically.

Enter proper values for the **Subnet Mask** and **Gateway Address** fields. Set the **Enable Ethernet Port** field to “y”, and select the appropriate **Network Region** for the C-LAN dedicated for AES connectivity. Default values may be used in the remaining fields. For the sample configuration, Network Region 1 is used. Submit these changes.

```
add ip-interface 1a02                                     Page 1 of 1
                                                         IP INTERFACES

      Type: C-LAN
      Slot: 01A02
      Code/Suffix: TN799 D
      Node Name: CLAN-01A02
      IP Address: 9 .1 .1 .8
      Subnet Mask: 255.255.255.0                               Link: 1
      Gateway Address: 9 .1 .1 .1
      Enable Ethernet Port? y                                Allow H.323 Endpoints? y
      Network Region: 1                                     Allow H.248 Gateways? n
      VLAN: n                                              Gatekeeper Priority: 1

Target socket load and Warning level: 400
Receive Buffer TCP Window Size: 8320
                                                         ETHERNET OPTIONS
      Auto? y
```

```
add ip-interface 1b02                                     Page 1 of 1
                                                         IP INTERFACES

      Type: C-LAN
      Slot: 01B02
      Code/Suffix: TN799 D
      Node Name: CLAN-01B02
      IP Address: 9 .1 .1 .9
      Subnet Mask: 255.255.255.0                               Link: 2
      Gateway Address: 9 .1 .1 .1
      Enable Ethernet Port? y                                Allow H.323 Endpoints? y
      Network Region: 1                                     Allow H.248 Gateways? n
      VLAN: n                                              Gatekeeper Priority: 1

Target socket load and Warning level: 400
Receive Buffer TCP Window Size: 8320
                                                         ETHERNET OPTIONS
      Auto? y
```

4.4. Administer Data Module for C-LAN

Add a new data module using the “add data-module n” command, where “n” is an available extension for each C-LAN module. Enter the following values:

- **Name:** A descriptive name
- **Type:** “ethernet”
- **Port:** Same slot number from **Section 4.3**, suffixed with port “17”
- **Link:** An available link number

```
add data-module 40000
                                DATA MODULE

Data Extension: 40000           Name: CLAN-01A02
      Type: ethernet
      Port: 01A0217
      Link: 1

Network uses 1's for Broadcast Addresses? Y
```

```
add data-module 49999
                                DATA MODULE

Data Extension: 49999           Name: CLAN-01B02
      Type: ethernet
      Port: 01b0217
      Link: 2

Network uses 1's for Broadcast Addresses? Y
```

4.5. Administer IP Services for AES Transport Link

Administer the transport link to the AES server with the “change ip-services” command. Add an entry with the following values for fields on **Page 1**:

- **Service Type:** “AESVCS”
- **Enabled:** “y”
- **Local Node:** C-LAN node name from **Section 4.2**
- **Local Port:** Retain the default value of “8765”

```
change ip-services
Page 1 of 4

Service      Enabled      Local      IP SERVICES      Remote      Remote
Type         y           Node       Local            Port        Node        Port
AESVCS       y           CLAN-01A02 8765
AESVCS       y           CLAN-01B02 8765
```

Proceed to **Page 4**, and enter the following values:

- **AE Services Server:** Name obtained from the AES server.
- **Password:** Same password to be administered on the AES server.
- **Enabled:** “y”

Note that the name and password entered for the **AE Services Server** and **Password** fields are case sensitive, and must match the name and password on the AES server. The administered name for the AES server is created as part of the AES installation, and can be obtained from the AES server by typing “uname -n” at the Linux command prompt. The same password entered in the screen below will need to be set on the AES server, as described in **Section 5.3**.

change ip-services				Page	4 of	4
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	govaes2	*	y			
2:						
3:						

4.6. Administer CTI Link for TSAPI Service

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. Submit these changes.

add cti-link 2		Page 1 of 3	
CTI LINK			
CTI Link: 2			
Extension: 55001			
Type: ADJ-IP			
		COR: 1	
Name: TSAPI GOVAES2			

4.7. Administer Stations for NICE

Add stations for use by the NiceLog recording channels. These are virtual stations that will be used by the NICE call recording system. It is assumed that the other stations that will be monitored by the NICE call recording system are already configured. There is a one-to-one mapping for the virtual station and the monitored station, i.e. one virtual station is needed for every monitored station. Both virtual and monitored stations extensions will be used later in **Section 5.5** and **Section 6.1 Step 12**.

Issue “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:** Enter station type “**4624**”.
- **Name:** A descriptive name.
- **Security Code:** Enter a valid code. All the NiceLog stations will use the same code.
- **COR:** Enter a COR which has “Can be Service Observed” and “Can be a Service Observer” enabled as “y”
- **IP SoftPhone:** “y”

add station 46001		Page 1 of 6
STATION		
Extension: 46001	Lock Messages? n	BCC: 0
Type: 4624	Security Code: 1234	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: NICE	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Personalized Ringing Pattern: 1	
Data Option: none	Message Lamp Ext: 46001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
	Media Complex Ext:	
	IP SoftPhone? y	

Proceed to **Page 2**, and set the **Multimedia Mode** to “enhanced”, **Auto Answer** to “none” and **Data Restriction** to “n”.

add station 46001		Page 2 of 6
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single	Conf/Trans on Primary Appearance? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed		
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	

On **Page 4**, assign the “conf-dsp” and “serv-obsrv” to any available buttons:

add station 46001		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	7:	
2: call-appr	8:	
3: call-appr	9:	
4: conf-dsp	10:	
5: serv-obsrv	11:	
6:	12:	

Repeat the “add station n” command to add the desired number of stations. For the compliance testing, eight virtual stations were administered which were used to monitor the corresponding stations.

NICE Virtual Stations	Monitored Stations
46001	23002
46002	41002
46003	51001
46004	51002
46005	52001
46006	52002
46007	53000
46008	53001

Note: The VDN and Agents-ID extensions do not require a virtual station.

4.8. Administer COR for Virtual and Monitored Stations

Issue “change cor n” command, where “n” is the COR number assigned to the virtual stations created in **Section 4.7**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Can Be Service Observed:** Enter “Y”.
- **Can Be A Service Observer:** Enter “Y”.

Note: All monitored stations also need the above values enabled in their respective COR forms.

4.9. Administer Feature Access code for Service Observing

Enter the “change feature-access-code” command. Navigate to **Page 5**, and set **Service Observing Listen Only Access Code**. This will be used in **Section 6.1 Step 8**.

```
change feature-access-codes                                     Page 5 of 9
                                FEATURE ACCESS CODE (FAC)

                                Automatic Call Distribution Features

                                After Call Work Access Code: *52
                                  Assist Access Code: *50
                                  Auto-In Access Code: *17
                                  Aux Work Access Code: *19
                                  Login Access Code: *15
                                  Logout Access Code: *16
                                  Manual-in Access Code: *18
                                Service Observing Listen Only Access Code: *30
                                Service Observing Listen/Talk Access Code: *31
                                  Service Observing No Talk Access Code: *32
                                  Add Agent Skill Access Code:
                                  Remove Agent Skill Access Code:
                                  Remote Logout of Agent Access Code:
```

4.10. Administer System Parameters

Enter the “change system-parameters features” command. Navigate to **Page 5**, and set **Create Universal Call ID (UCID)** to “y” and **UCID Network Node ID** to an unassigned node ID.

```
change system-parameters features                             Page 5 of 17
                                FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                      Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name:
                                Emergency Extension Forwarding (min): 10
                                Enable Inter-Gateway Alternate Routing? n
                                Enable Dial Plan Transparency in Survivable Mode? n
                                COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
                                Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:

SEND ALL CALLS OPTIONS
                                Send All Calls Applies to: station    Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
                                Create Universal Call ID (UCID)? y    UCID Network Node ID: 123
```

Navigate to **Page 6**, and set **Conference Tone** and **Intrusion Tone** to “n”.

change system-parameters features	Page 6 of 17
FEATURE-RELATED SYSTEM PARAMETERS	
Public Network Trunks on Conference Call: 5	Auto Start? n
Conference Parties with Public Network Trunks: 6	Auto Hold? y
Conference Parties without Public Network Trunks: 6	Attendant Tone? y
Night Service Disconnect Timer (seconds): 180	Bridging Tone? n
Short Interdigit Timer (seconds): 3	Conference Tone? n
Unanswered DID Call Timer (seconds):	Intrusion Tone? n
Line Intercept Tone Timer (seconds): 30	Mode Code Interface? y
Long Hold Recall Timer (seconds): 0	
Reset Shift Timer (seconds): 0	
Station Call Transfer Recall Timer (seconds): 0	Recall from VDN? n
DID Busy Treatment: tone	

Navigate to **Page 13**, and set **Send UCID to ASAI** to “y”.

change system-parameters features	Page 13 of 17
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER MISCELLANEOUS	
Clear Callr-info: next-call	
Allow Ringer-off with Auto-Answer? n	
Reporting for PC Non-Predictive Calls? n	
ASAI	
Copy ASAI UUI During Conference/Transfer? n	
Call Classification After Answer Supervision? n	
Send UCID to ASAI? Y	

5. Configure Avaya Application Enablement Services

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

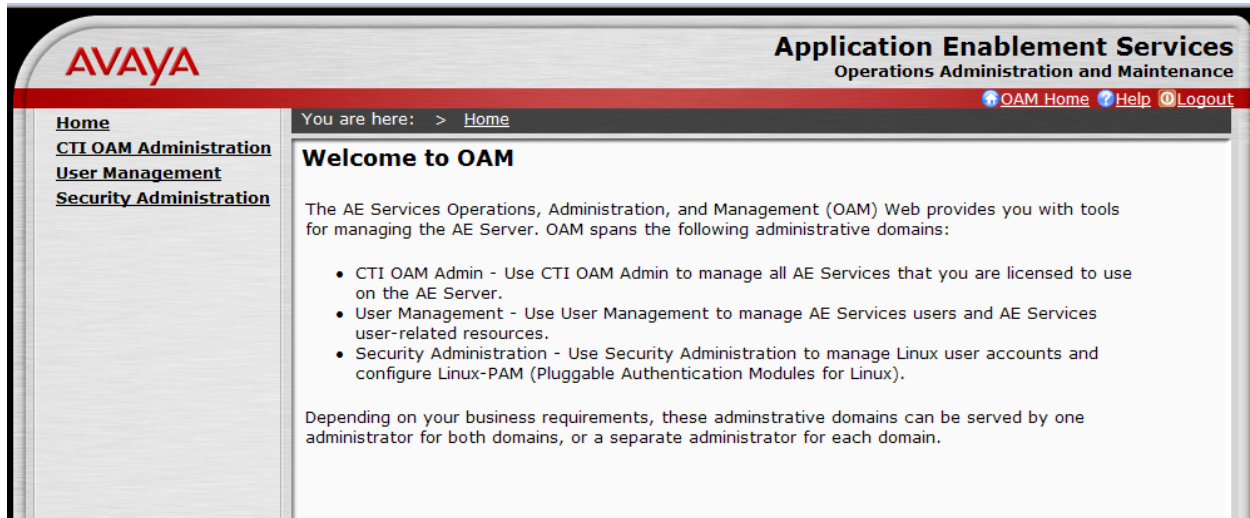
- Verify Avaya Application Enablement Services License
- Administer local IP
- Administer switch connection
- Administer TSAPI link
- Administer security database
- Obtain Tlink name
- Administer NICE users
- Administer device groups
- Restart TSAPI service

5.1. Verify Avaya Application Enablement Services License

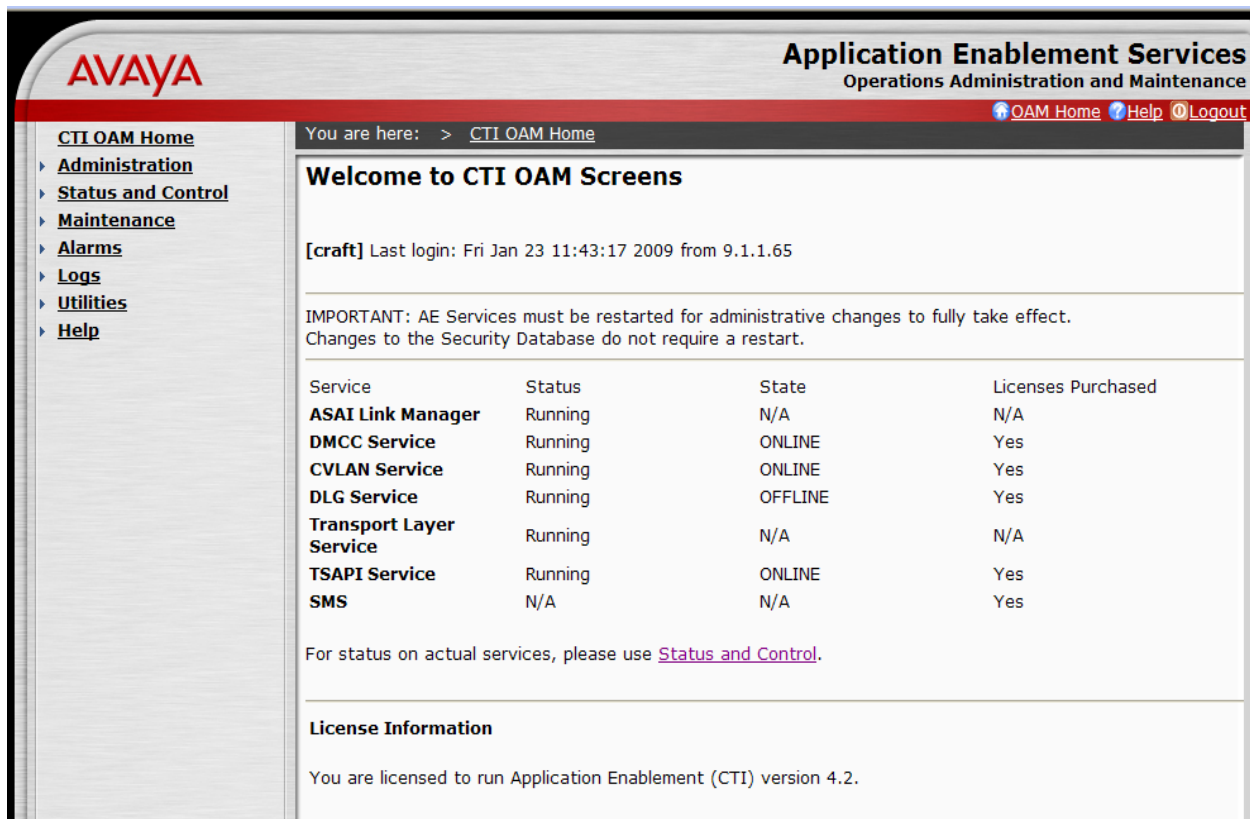
Access the AES OAM web based interface by using the URL “https://ip-address:8443/MVAP” in an Internet browser window, where “ip-address” is the IP address of the AES server. The **Login** screen is displayed as shown below. Note that the AES OAM includes two separate administrative accounts, one to access CTI OAM Admin and a separate one to access User Management. Log in using the CTI OAM Admin user name and password.



The **Welcome to OAM** screen is displayed, as shown below. Select **CTI OAM Administration** from the left pane.



The **Welcome to CTI OAM Screens** is displayed. Verify that AES is licensed for the TSAPI service, as shown below. If the TSAPI service is not licensed, contact the Avaya sales team or business partner for a proper license file.



5.2. Administer Local IP

Select **Administration > Network Configuration > Local IP** from the left pane. The **Local IP** screen is displayed into the right pane, as shown below. In the **Client Connectivity** field, select the AES server IP address that will be used to interface to NICE Call Recording system. In the **Switch Connectivity** field, select the AES server IP address that will be used to connect to Avaya Communication Manager. In the sample configuration, the same NIC interface is used for the Client Connectivity and Switch Connectivity. Note that in some cases, they might be different. Click on **Apply Changes**.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The left pane contains a navigation menu with the following items: CTI OAM Home, Administration (expanded), Network Configuration (expanded), Local IP (selected), NIC Configuration, Ports, Switch Connections, CTI Link Admin, and DMCC Configuration. The right pane displays the 'Local IP' configuration screen. At the top, it says 'You are here: > Administration > Network Configuration > Local IP'. Below this, there are three dropdown menus: 'Client Connectivity' with 'eth0:9.1.1.51' selected, 'Switch Connectivity' with 'eth0:9.1.1.51' selected, and 'Media Connectivity' with 'eth0:9.1.1.51' selected. An 'Apply Changes' button is located at the bottom of the configuration area.

5.3. Administer Switch Connection

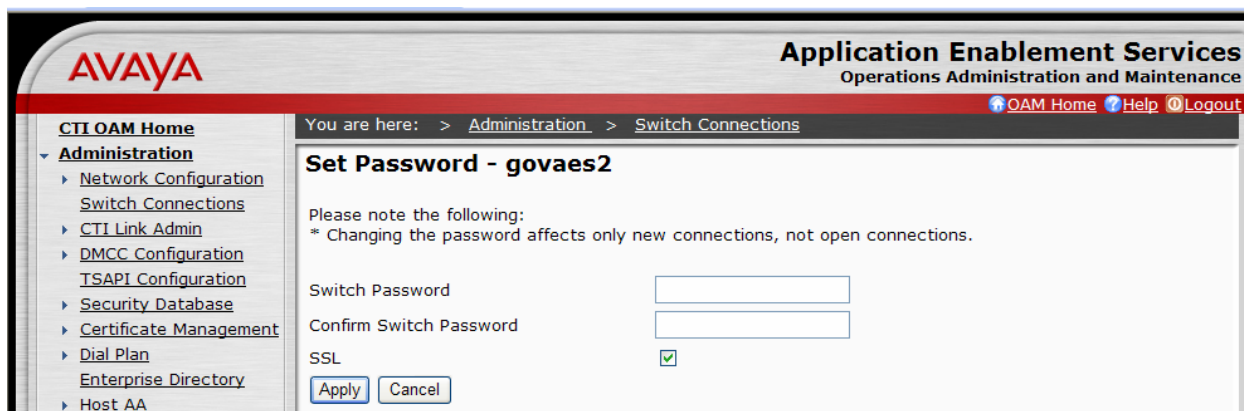
Select **Administration > Switch Connections** from the left pane. The **Switch Connections** screen is displayed, as shown below. Enter a descriptive name for the switch connection and click on **Add Connection**. In this case, “govaes2” is used. Note that the actual switch connection name may vary.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The left pane contains a navigation menu with the following items: CTI OAM Home, Administration (expanded), Network Configuration, Switch Connections (selected), CTI Link Admin, and DMCC Configuration. The right pane displays the 'Switch Connections' screen. At the top, it says 'You are here: > Administration > Switch Connections'. Below this, there is a text input field and an 'Add Connection' button.

Next, the **Set Password – govaes2** screen is displayed. Enter the following values for the specified fields:

- **Switch Password:** Same password from **Section 4.5**.
- **Confirm Switch Password:** Re-enter the same password from **Section 4.5**.
- **SSL:** Retain the check.

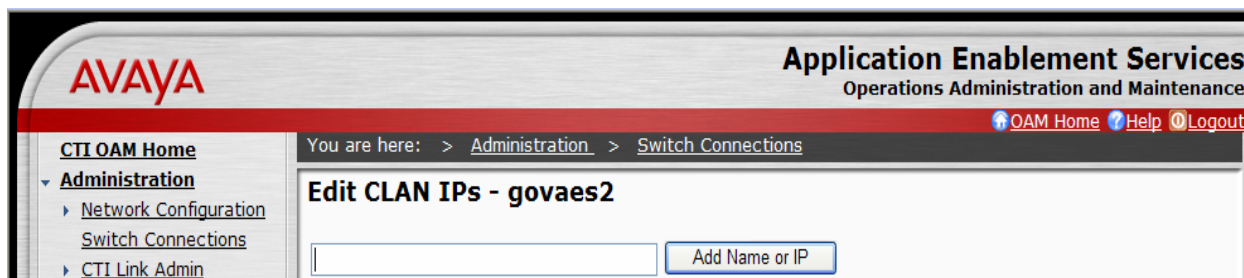
Click on **Apply**.



The **Switch Connections** screen is displayed next, as shown below. Select the newly added switch connection name from the listing, and click on **Edit CLAN IPs**.

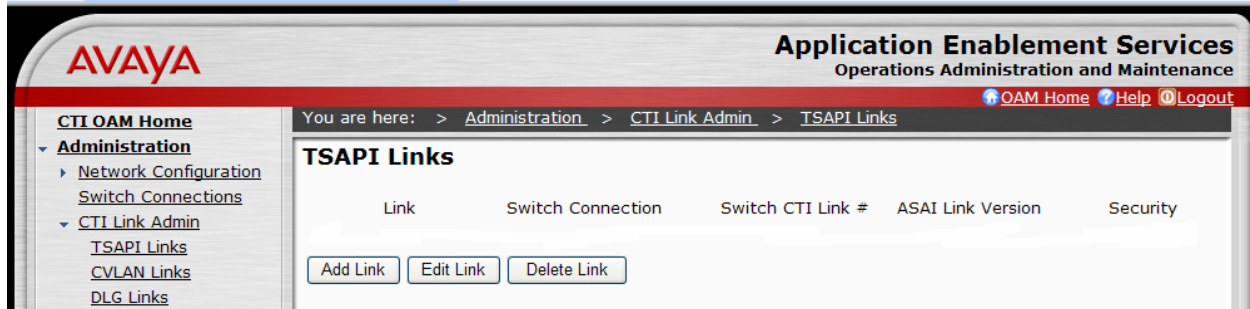


The **Edit CLAN IPs – govaes2** screen is displayed next. Enter the host name or IP address of the C-LAN used for AES connectivity from **Section 4.2**. Click on **Add Name or IP**. In the sample configuration two C-LANs will be administered.

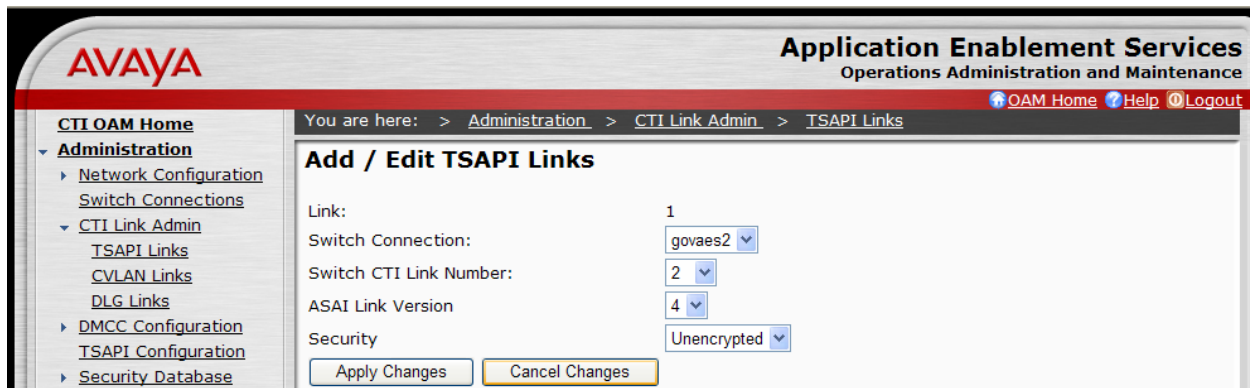


5.4. Administer TSAPI Link

To administer a TSAPI link, select **Administration > CTI Link Admin > TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click on **Add Link**.



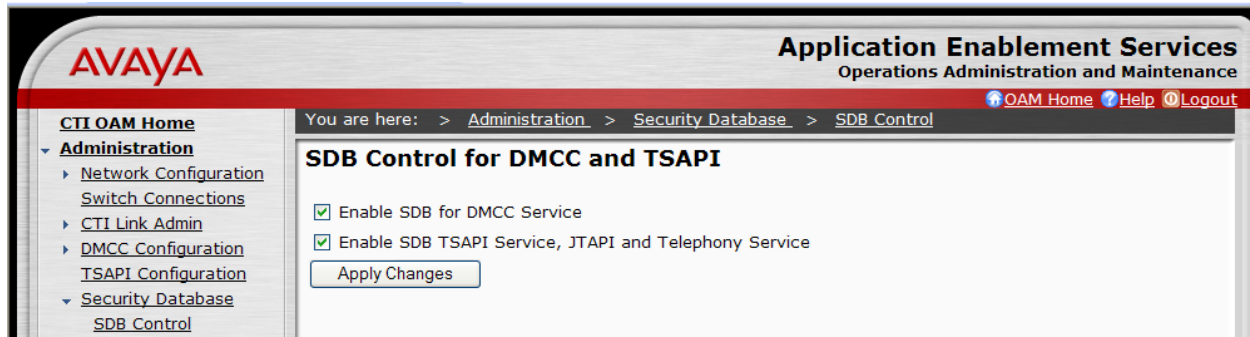
The **Add / Edit TSAPI Links** screen is displayed next. The **Link** field is only local to the AES server, and may be set to any available number. For **Switch Connection**, select the name of the switch connection from **Section 5.3**. For **Switch CTI Link Number**, select the CTI link number from **Section 4.6**. Accept the default values for **ASAI Link Version** and **Security**. Click on **Apply Changes**.



The **Apply Changes to Link** screen is displayed (not shown). Click on **Apply**.

5.5. Administer Security Database

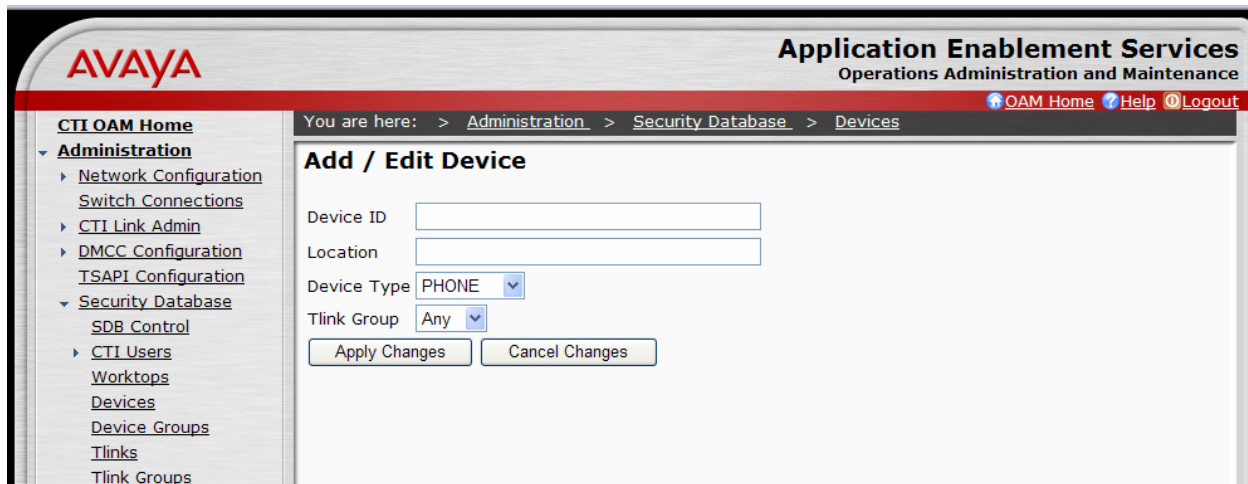
Enable the security database on AES, as this functionality is utilized by NICE. Select **Administration > Security Database > SDB Control** to display the **SDB Control for DMCC and TSAPI** screen shown below. Click on **Enable SDB for DMCC Service** and **Enable SDB TSAPI Service, JTAPI and Telephony Service**. Click on **Apply Changes**.



All devices that are monitored by NICE need to be configured in the AES security database. These include all the virtual stations that were created in **Section 4.7** and also the station extensions which will be monitored by NICE call recording.

Select **Administration > Security Database > Devices**, and add each device by entering the device extension and clicking on **Add Device**.

The **Add / Edit Device** screen is used to enter the associated field values for each device, as shown below. Only enter the Device Type as PHONE in this list. This should include both the virtual stations administered in **Section 4.7** and the corresponding monitored stations.



A sample listing of the configured devices used for the compliance testing is shown below. Note that the total number of devices may vary, as this depends on the number of extensions to be monitored and controlled. The list below contains all the devices (PHONE, VDN and AGENT ID) administered on the AES. Not all these devices will be used by NICE. Only selected devices will be administered for the NICE Device Group, as described in **Section 5.8**.

Application Enablement Services
Operations Administration and Maintenance

[OAM Home](#)
[Help](#)
[Logout](#)

You are here: > [Administration](#) > [Security Database](#) > [Devices](#)

CTI OAM Home

- Administration
 - Network Configuration
 - Switch Connections
 - CTI Link Admin
 - DMCC Configuration
 - TSAPI Configuration
 - Security Database
 - SDB Control
 - CTI Users
 - Worktops
 - Devices
 - Device Groups
 - Tlinks
 - Tlink Groups
 - Certificate Management
 - Dial Plan
 - Enterprise Directory
 - Host AA
 - SMS Configuration
 - WebLM Configuration
 - Bridged Alert Config
- Status and Control
- Maintenance
- Alarms
- Logs
- Utilities
- Help

Devices

	Device ID	Tlink Group	Device Type	Location
<input checked="" type="radio"/>	0000000000000000	Any	PHONE	
<input type="radio"/>	23002	Any	PHONE	Digital Phone
<input type="radio"/>	41002	Any	PHONE	Analog Phone
<input type="radio"/>	46001	Any	PHONE	NICE Virtual Station
<input type="radio"/>	46002	Any	PHONE	NICE Virtual Station
<input type="radio"/>	46003	Any	PHONE	NICE Virtual Station
<input type="radio"/>	46004	Any	PHONE	NICE Virtual Station
<input type="radio"/>	46005	Any	PHONE	NICE Virtual Station
<input type="radio"/>	46006	Any	PHONE	NICE Virtual Station
<input type="radio"/>	46007	Any	PHONE	NICE Virtual Station
<input type="radio"/>	46008	Any	PHONE	NICE Virtual Station
<input type="radio"/>	49010	Any	AGENT ID	PlantCML Agent1
<input type="radio"/>	49011	Any	AGENT ID	PlantCML Agent2
<input type="radio"/>	51001	Any	PHONE	IP Phone (Mayor's Office)
<input type="radio"/>	51002	Any	PHONE	IP Phone (PSAP Supervisor)
<input type="radio"/>	52001	Any	PHONE	Lincroft EMT (SIP radio endpoint)
<input type="radio"/>	52002	Any	PHONE	Lincroft Police (SIP radio endpoint)
<input type="radio"/>	53000	Any	PHONE	PlantCML (46XX IP Phone)
<input type="radio"/>	53001	Any	PHONE	PlantCML (96XX IP Phone)
<input type="radio"/>	53002	Any	PHONE	PlantCML (46xx, NOT monitored by NICE)
<input type="radio"/>	53003	Any	PHONE	Plantcml (96xx, NOT monitored by NICE)
<input type="radio"/>	53015	Any	VDN	PlantCML VDN 1
<input type="radio"/>	53020	Any	VDN	PlantCML VDN 2

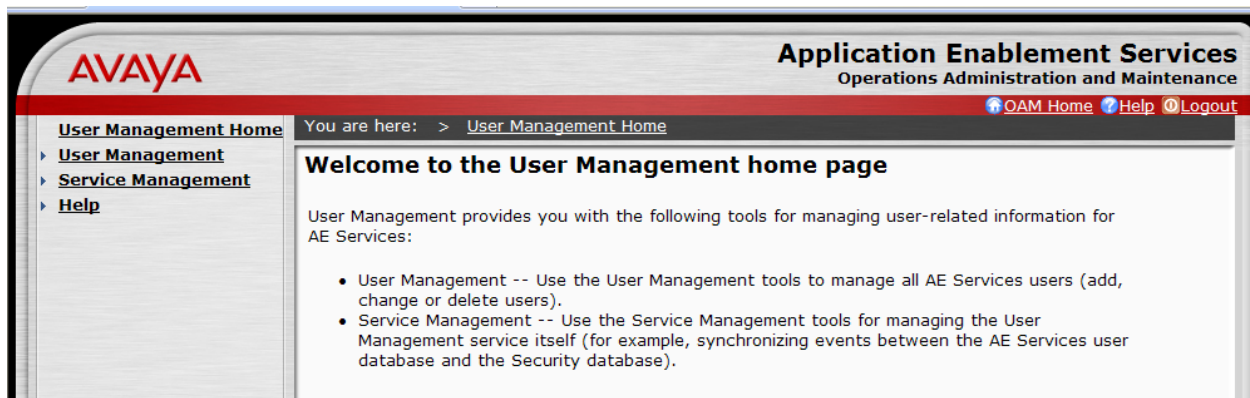
5.6. Obtain Tlink Name

Select **Administration > Security Database > Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated by the AES server, upon creation of a new switch connection. Locate the Tlink Name associated with the newly created switch connection, which would utilize the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring the NICE server in **Section 6.1 Step 7**.



5.7. Administer NICE Users

Administer an user account for the NICE server. Follow the login procedures in **Section 5.1**, and log in with the User Management user name and password. The **Welcome to the User Management home page** screen is displayed, as shown below.



Select **User Management > Add User** from the left pane. In the **Add User** screen shown below, enter values for the **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password** fields to create a user account for the NICE server. Retain the default value of “None” for **Avaya Role**, and select “Yes” from the **CT User** drop-down list. Click on **Apply** at the bottom of the screen (not shown below). Make a note of the User Id and Password, to be used later for configuring the NICE server in **Section 6.1 Step 7**

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

Csx Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

Home Phone

Home Postal Address

Follow the login procedures in **Section 5.1**, and log in with the CTI OAM Admin user name and password. Select **Administration > Security Database > CTI Users > List All Users** to get a listing of all CTI users, as shown below.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > [Administration](#) > [Security Database](#) > [CTI Users](#) > [List All Users](#)

CTI Users

	User ID	Common Name	Worktop Name	Device ID
<input type="radio"/>	49010	Agent1	NONE	NONE
<input type="radio"/>	49011	Agent2	NONE	NONE
<input type="radio"/>	cmapi	PlantCML	NONE	NONE
<input checked="" type="radio"/>	nice	nice	NONE	NONE
<input type="radio"/>	sentinel	Sentinel	NONE	NONE

5.8. Administer Device Groups

Administer a device group to be used by NICE, to control user access of devices. Select **Administration > Security Database > Device Groups** from the left pane. In the **Device Groups** screen shown below, enter a descriptive value, and click on **Add Device Group**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > [Administration](#) > [Security Database](#) > [Device Groups](#)

Device Groups

Device Group Exception Group?

For the sample configuration, a device group of “NICE” was created. Click on **Edit Device Group**. The **Add / Edit Device Group** screen is displayed, as shown below. Select all devices that were created in **Section 5.5**, and click on **Apply Changes**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Security Database > Device Groups

Add / Edit Device Group

Device Group:

Exception Group: ☐

Devices

<input checked="" type="checkbox"/>	0000000000000000
<input checked="" type="checkbox"/>	23002
<input checked="" type="checkbox"/>	41002
<input checked="" type="checkbox"/>	46001
<input checked="" type="checkbox"/>	46002
<input checked="" type="checkbox"/>	46003
<input checked="" type="checkbox"/>	46004
<input checked="" type="checkbox"/>	46005
<input checked="" type="checkbox"/>	46006
<input checked="" type="checkbox"/>	46007
<input checked="" type="checkbox"/>	46008
<input type="checkbox"/>	49010
<input type="checkbox"/>	49011
<input checked="" type="checkbox"/>	51001
<input checked="" type="checkbox"/>	51002
<input checked="" type="checkbox"/>	52001
<input checked="" type="checkbox"/>	52002
<input checked="" type="checkbox"/>	53000
<input checked="" type="checkbox"/>	53001
<input type="checkbox"/>	53002
<input type="checkbox"/>	53003
<input type="checkbox"/>	53015
<input type="checkbox"/>	53020

Apply Changes Select All Deselect All Cancel Changes

The **Apply Changes to Device Group Properties** screen is displayed next. Click on **Apply** to confirm the changes.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Security Database > Device Groups

Apply Changes to Device Group Properties

Warning! Are you sure you want to apply the changes?

Apply Cancel

Select **Administration > Security Database > CTI Users > List All Users** to view the listing of all CTI users again, as shown below. Select the user ID created for the NICE server, and click on **Edit**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Security Database > CTI Users > List All Users

CTI Users

	User ID	Common Name	Worktop Name	Device ID
<input type="radio"/>	49010	Agent1	NONE	NONE
<input type="radio"/>	49011	Agent2	NONE	NONE
<input type="radio"/>	cmapi	PlantCML	NONE	NONE
<input checked="" type="radio"/>	nice	nice	NONE	NONE
<input type="radio"/>	sentinel	Sentinel	NONE	NONE

[Edit](#) [List All](#)

The **Edit CTI User** screen is displayed, as shown below. Select the newly created device group for the **Call Origination and Termination, Device / Device, Call / Device, and Allow Routing on Listed Device** fields. Click on **Call / Call**, followed by **Apply Changes**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Security Database > CTI Users > List All Users

Edit CTI User

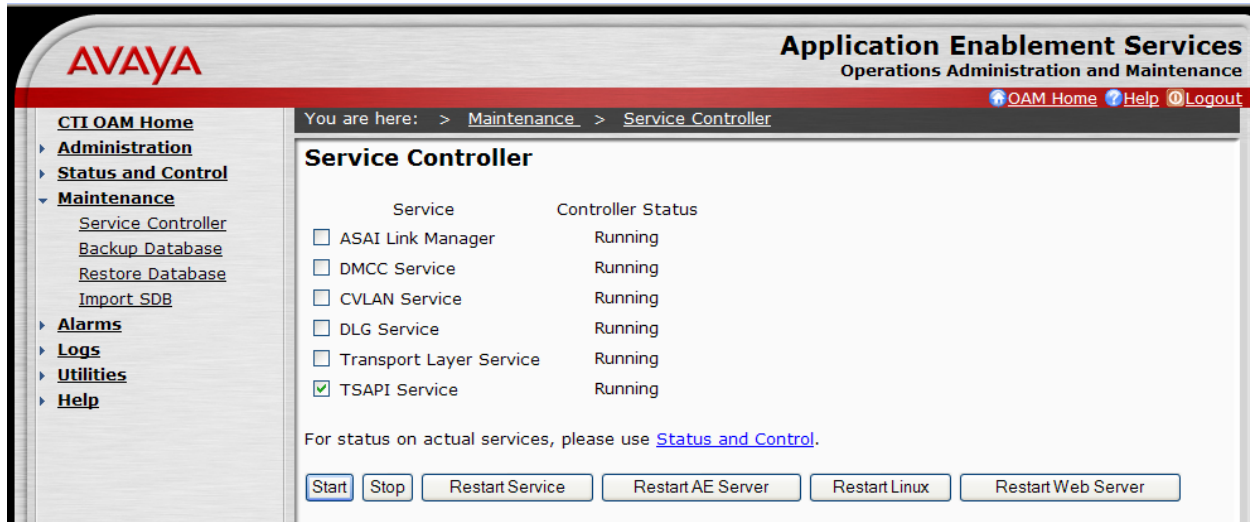
User ID: nice
Common Name: nice
Worktop Name: NONE
Unrestricted Access: Enable

Call Origination and Termination: NICE
Device / Device: NICE
Call / Device: NICE
Call / Call: ☒
Allow Routing on Listed Device: NICE

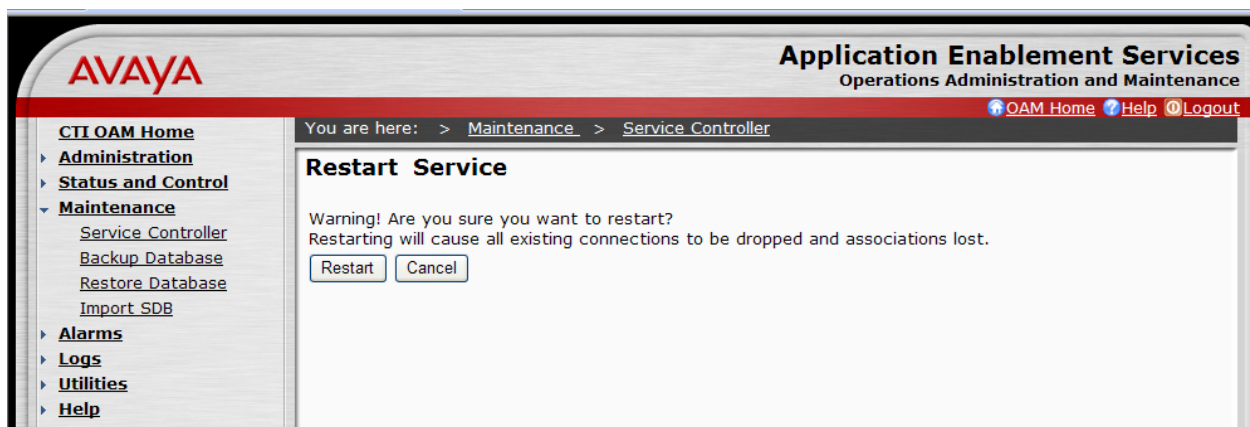
[Apply Changes](#) [Cancel](#)

5.9. Restart TSAPI Service

Select **Maintenance > Service Controller**. The **Service Controller** screen shows a listing of the services and associated status. Check the **TSAPI Service**, and click on **Restart Service**.



The following **Restart Service** screen is displayed. Click on **Restart** to confirm the restart.

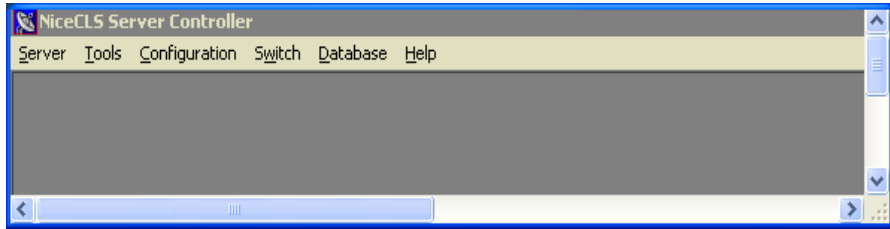
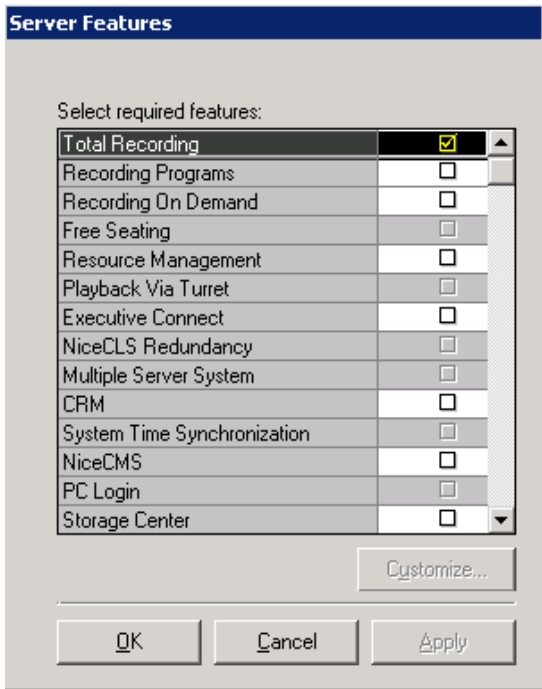


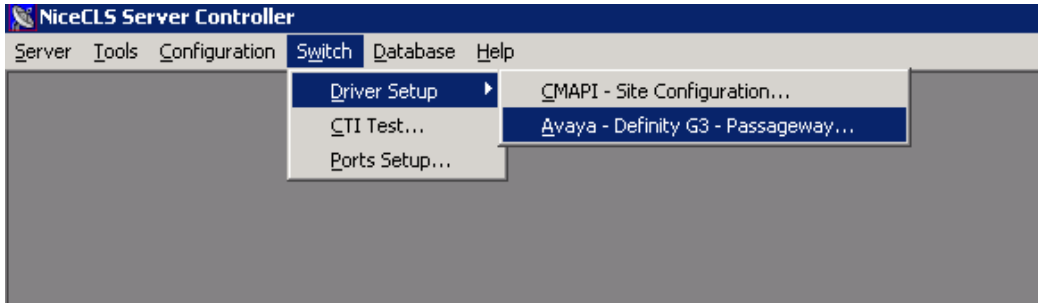
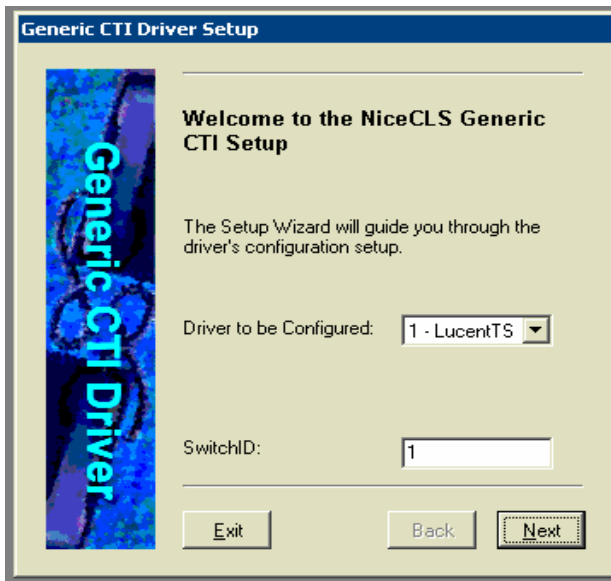
6. Configure NICE Call Recording System

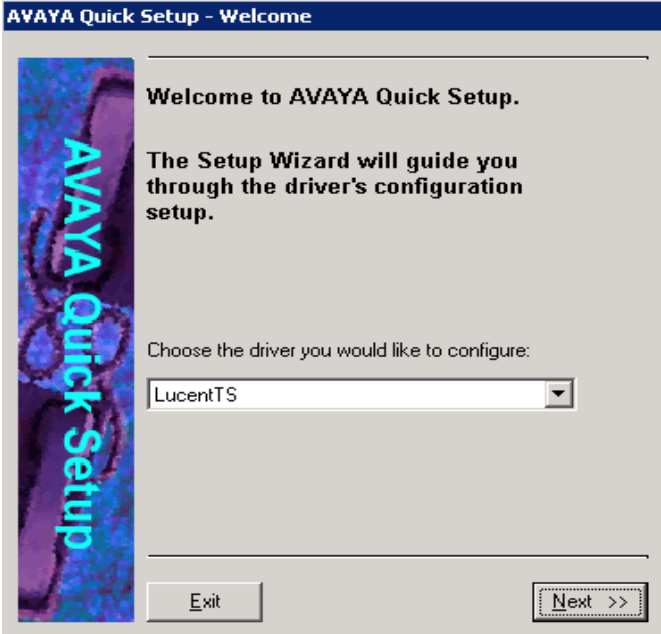
These Application Notes assume that the NICE call recording system depicted in **Figure 2** is already installed. Refer to [3] for detailed information about the installation procedure. It is also assumed that the Avaya AES 4.2.1 TSAPI Client application is already installed on the NICE server. Refer to [1] for detailed information.

6.1. Configure NiceCLS server

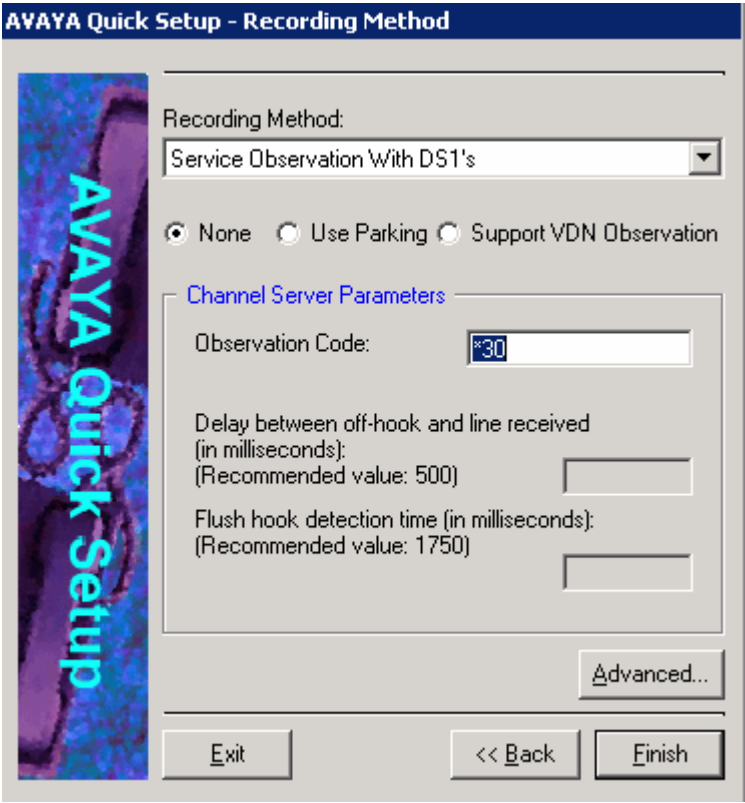
The steps in this section describe the system configuration of the NiceCLS server. For detailed NiceCLS configuration information, please refer to [3].

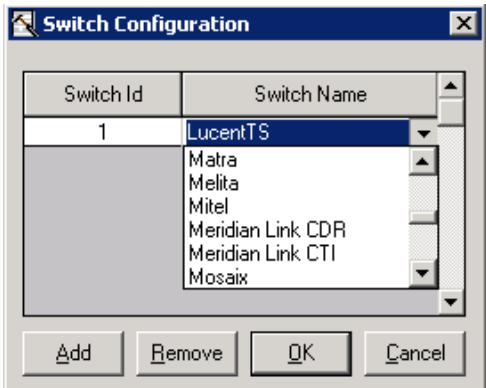
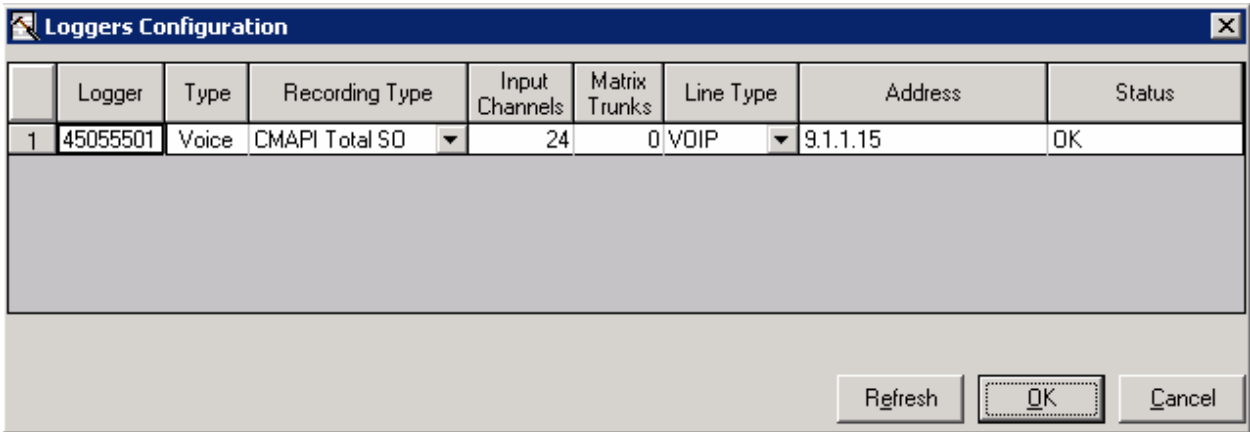
Step	Description
1.	<p>On the NiceCLS server, launch the NiceCLS Server Controller by navigating to Programs → NiceCLS Server 8.93 → NiceCLS Server Controller.</p> 
2.	<p>In the NiceCLS Server Controller window, click on Configuration → Server Features. The Server Features screen appears. Check the Total Recording. Click OK.</p> 

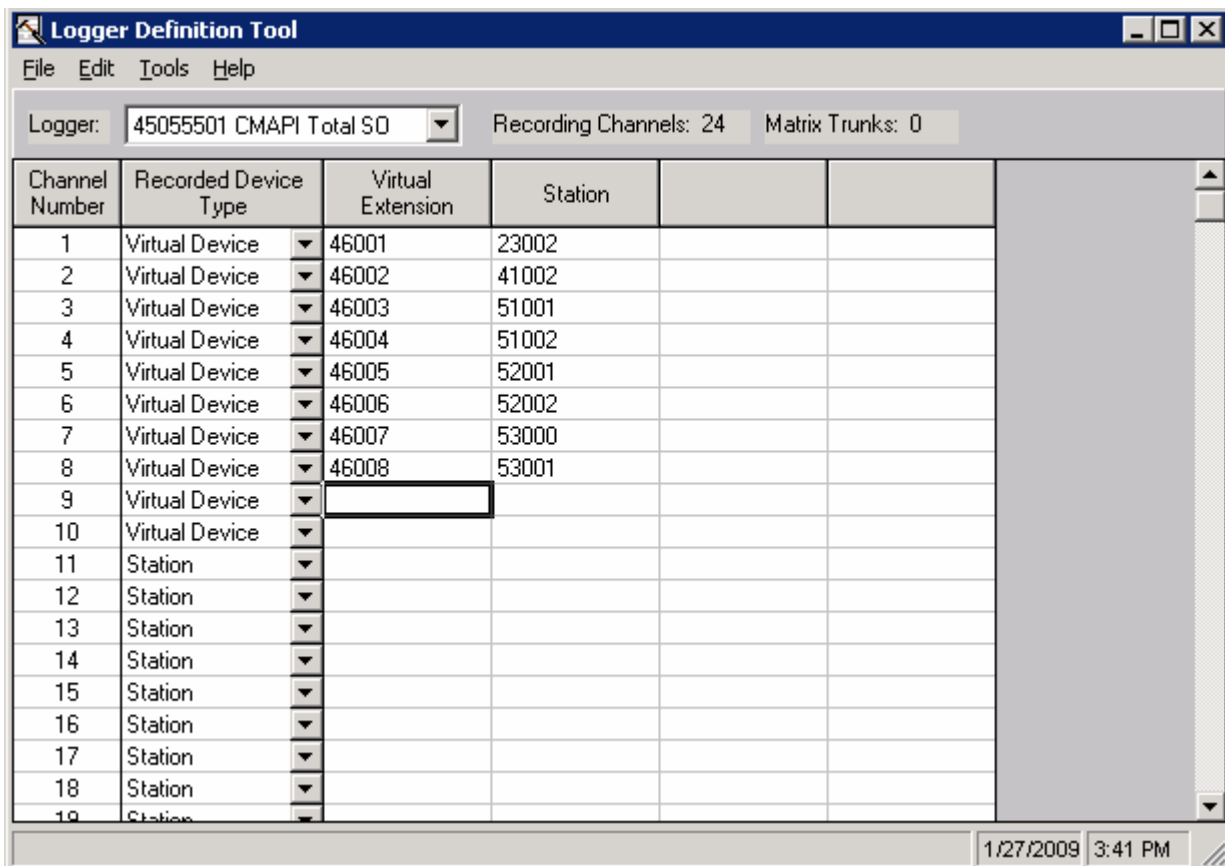
Step	Description
3.	<p>In the NiceCLS Server Controller window, click on Switch → Driver Setup → Avaya-Definity G3-Passageway..</p>  <p>The Generic CTI Driver Setup screen appears. Enter the following values, and then click Next.</p> <ul style="list-style-type: none"> • Driver to be Configured: Select “1- LucentTS” from the drop down list. • SwitchID: Retain the default value “1”. This value will be used in Step 16. 
4.	The Generic CTI Driver Features screen appears. Click Next .
5.	The Devices Mapping screen appears. Click Finish .

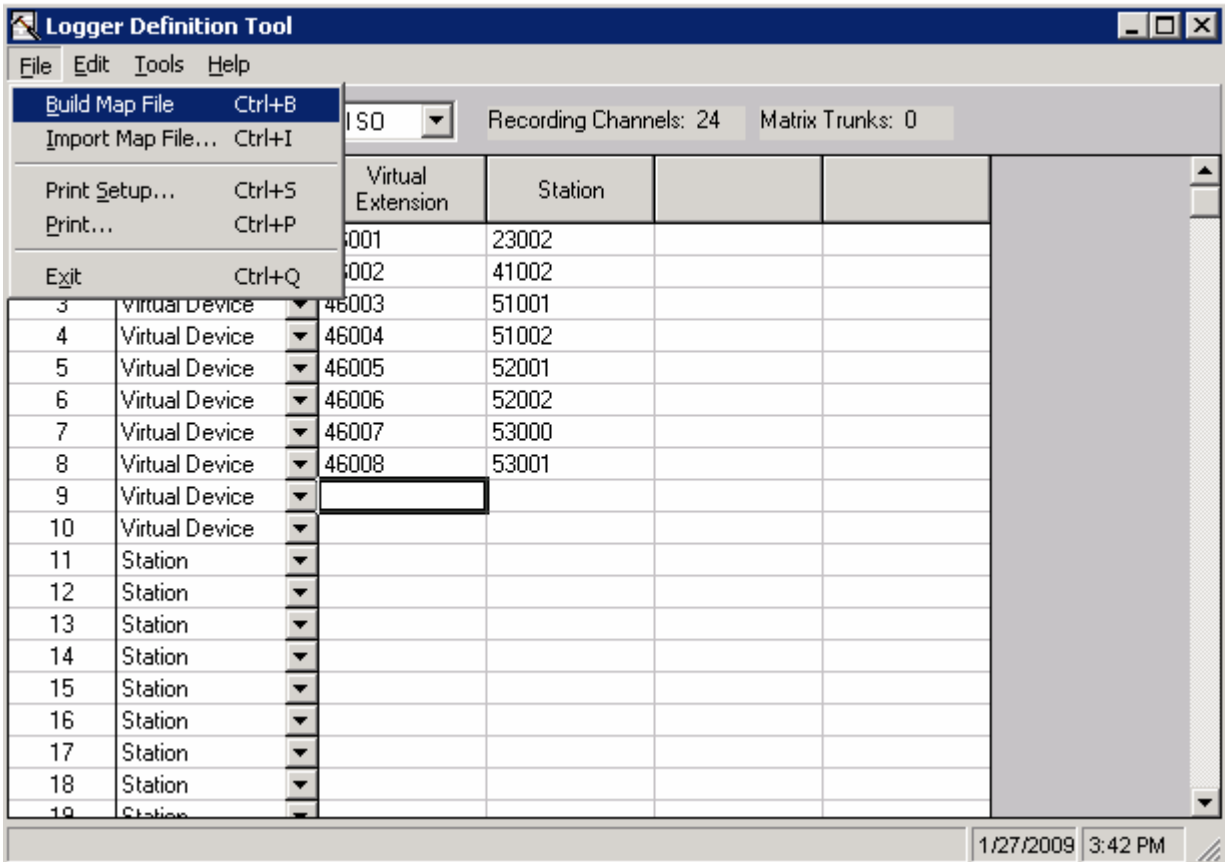
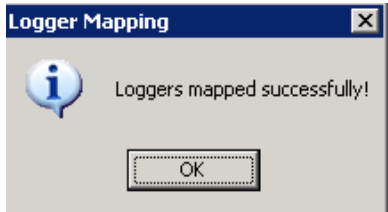
Step	Description
6.	<p>The AVAYA Quick Setup – Welcome screen appears. Select “LucentTS” from the Choose the driver you would like to configure drop down list, and then click Next.</p> 

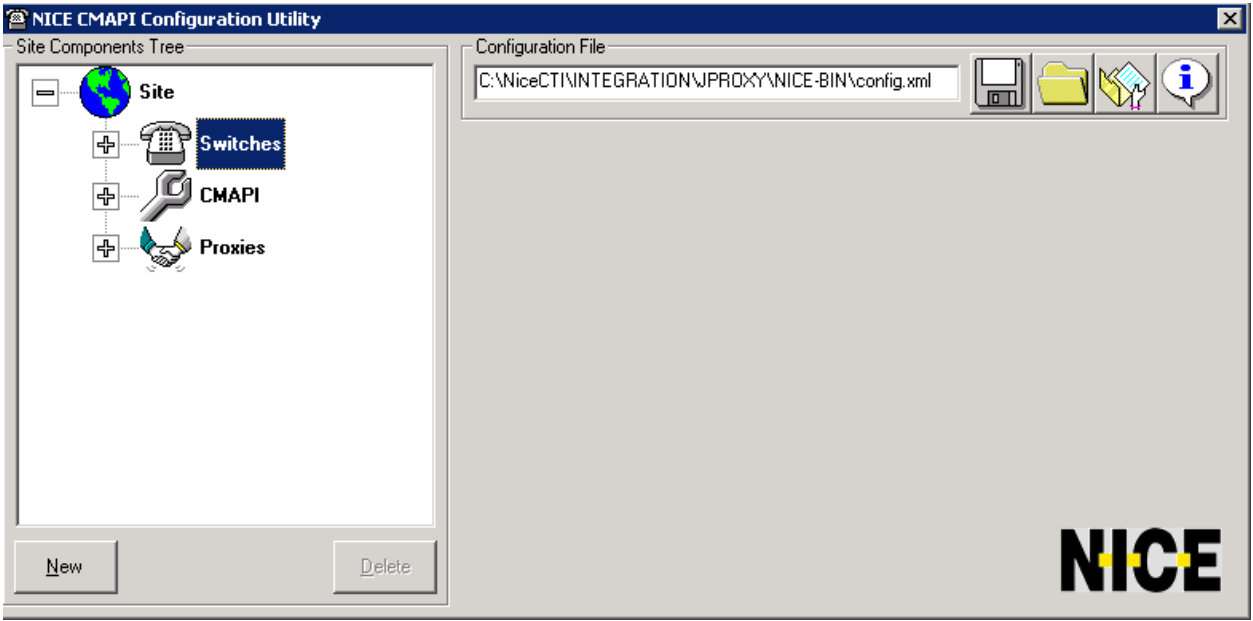
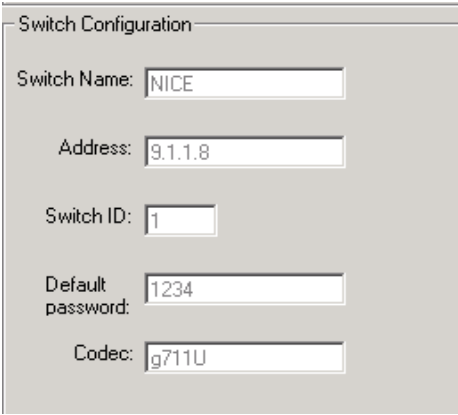
Step	Description
7.	<p>Select “AVAYA#GOVAES2#CSTA#GOVAES2” from the Select Server drop down list. The Select Server information was created after performing configuration in Section 5.6. Enter the login ID and password administered in Section 5.7.</p> <div data-bbox="578 369 1234 1043" data-label="Image"> </div> <p>Click Test Connection.</p> <div data-bbox="600 1155 1208 1377" data-label="Image"> </div> <p>Click OK.</p>

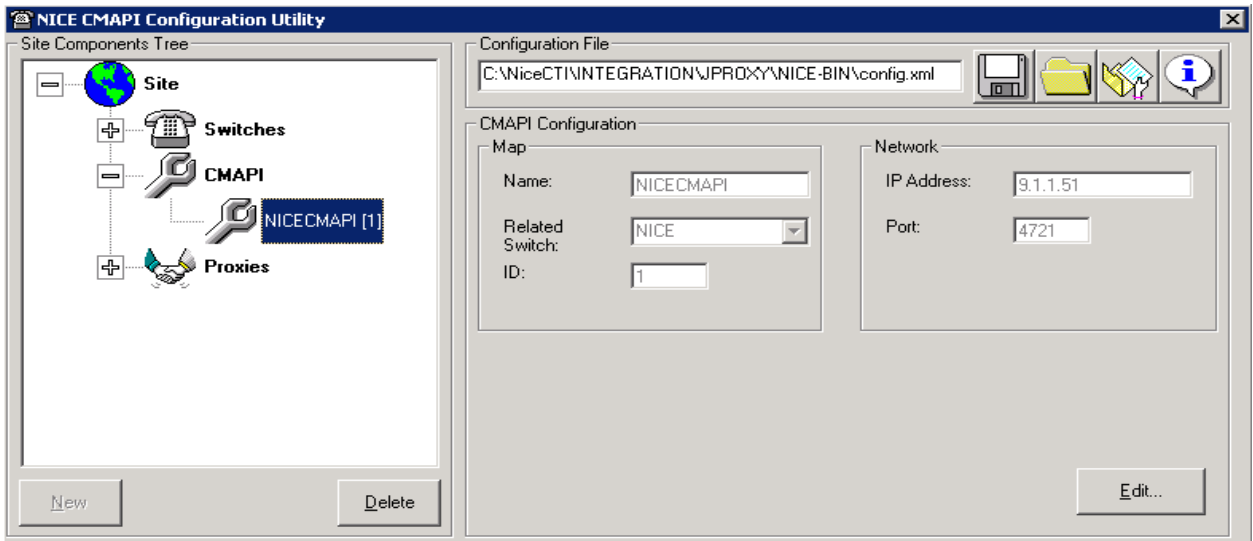
Step	Description
8.	<p>The AVAYA Quick Setup – Recording Method screen appears. Select “Service Observation with DS1’s” from the Recording Method drop down list. Enter the administered feature access code for Service Observing from Section 4.9 and then click Finish.</p> 
9.	<p>In the NiceCLS Server Controller, click on Configuration → Logger Definition Tool. The Logger Definition Tool screen appears. In the Logger Definition Tool, click on Edit → Switches.</p>

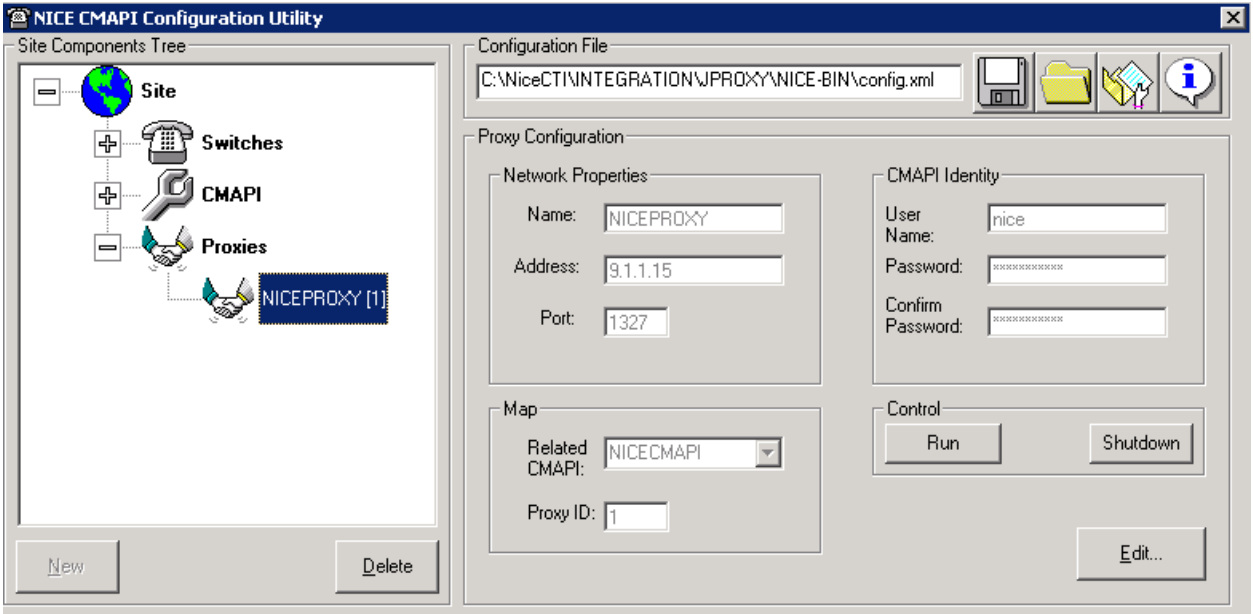

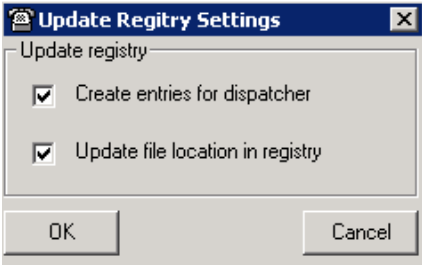
Step	Description
10.	<p>The Switch Configuration screen appears. From the Switch Name drop down list, select “LucentTS”, and then click OK.</p> 
11.	<p>In the Logger Definition Tool, click on Edit → Loggers. The Logger Configuration screen appears. Enter the following values, and then click OK.</p> <ul style="list-style-type: none"> • Recording Type: Select “CMAPI Total SO” (Service Observing). • Input Channels: Enter the number of stations that will be recorded. • Line Type: Select “VOIP” from the Line Type drop down list. • Address: Select the default value. • Status: Select the default value. 


Step	Description
12.	<p>In the Logger Definition Tool, enter the following values, and then click OK.</p> <ul style="list-style-type: none"> • Recorded Device Type: Select “Virtual Device” from the drop down list. • Virtual Extension: Enter the IP Softphone extension administered in Section 4.7. • Station: Enter the monitored station extension number. 

Step	Description
13.	<p>In the Logger Definition Tool, click on File → Build Map File.</p> 
14.	<p>The Logger Mapping screen appears. Click OK to confirm the change.</p> 

Step	Description
15.	<p>From the NiceCLS Server Controller, click on Switch → Driver Setup → CMAPI - Site Configuration. The NICE CMAPI Configuration Utility screen appears. Click on Switches, and then click New.</p> 
16.	<p>The Switch Configuration screen appears. Enter the following values, and then click OK.</p> <ul style="list-style-type: none"> • Switch Name: A descriptive name, for example NICE. • CLAN Board IP Address: The C-LAN IP address administered in Section 4.3. Enter only one C-LAN IP address. • Switch ID: Enter the switch ID “1”. The value administered in Step 3. • Default Password: The security code administered in Section 4.7. • Codec: Select g711U. 

Step	Description
17.	<p>In the NICE CMAPI Configuration Utility, click on CMAPI, and then click New (not shown). The New CMAPI Properties screen appears. Enter the following values, and then click OK.</p> <ul style="list-style-type: none"> • Name: A descriptive name. • ID: Enter the AES server ID “1”. • Related Switch: Select “NICE” which was entered in Step 16. • IP Address: Enter the AES server IP address. • Port: Retain the default value “4721”.
	<p>The updated screen is shown below:</p>
	



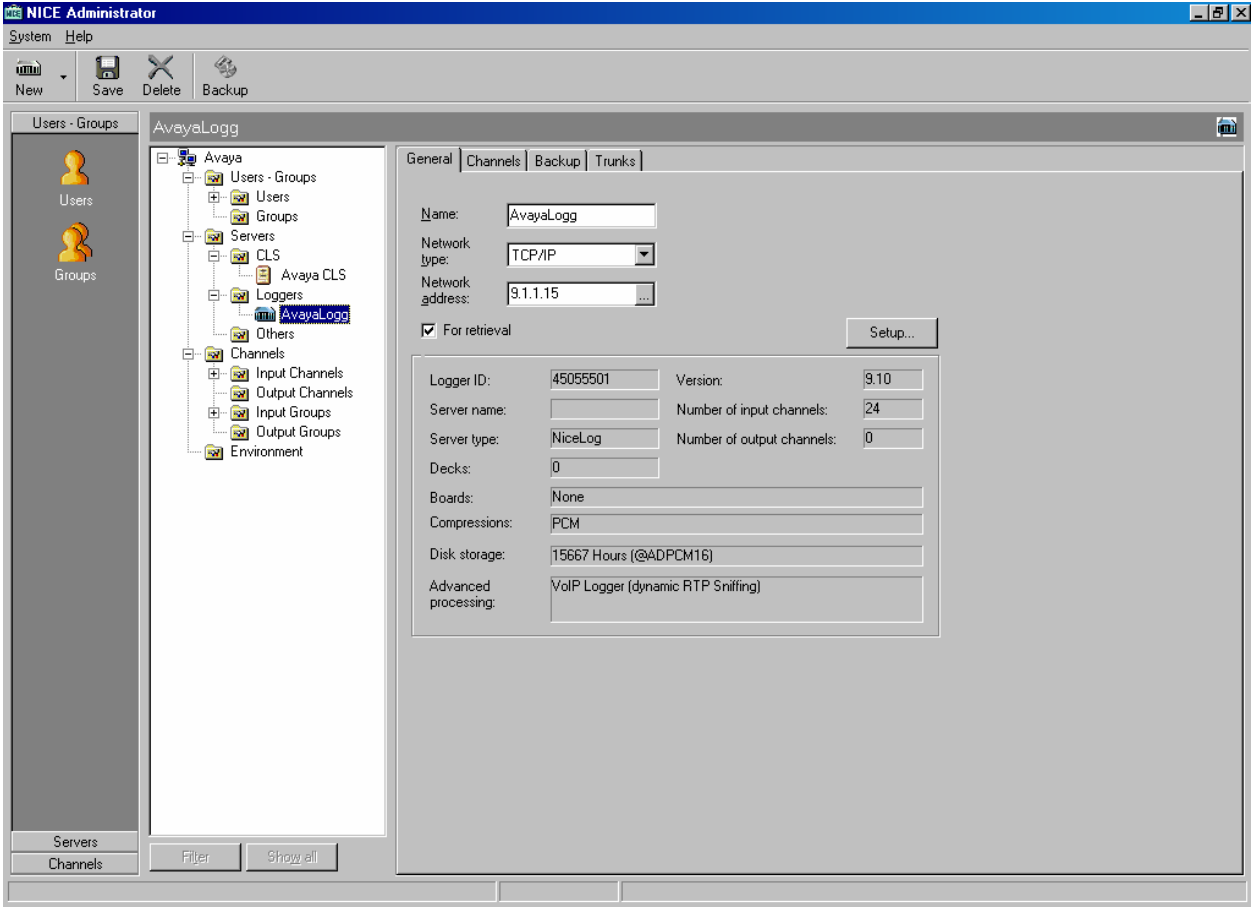
Step	Description
18.	<p>From the NICE CMAPI Configuration Utility, click on Proxies, and then click New (not shown). The New Proxy Properties screen appears. Enter the following values, and then click OK.</p> <ul style="list-style-type: none"> • Name: A descriptive name. • Address: Enter the local IP address of the NICE call recording system (9.1.1.15). • Port: Retain the default value “1327”. • Related CMAPI: Select “NICECMAPI”, which was entered in Step 17. • Proxy ID: Enter a unique ID, for example 1. <p>The updated screen is shown below:</p> 
19.	<p>In the NICE CMAPI Configuration Utility, click on Save . The Update Registry Settings window appears. Check the Create entries for dispatcher and Update file location in registry checkboxes. Click OK.</p> 


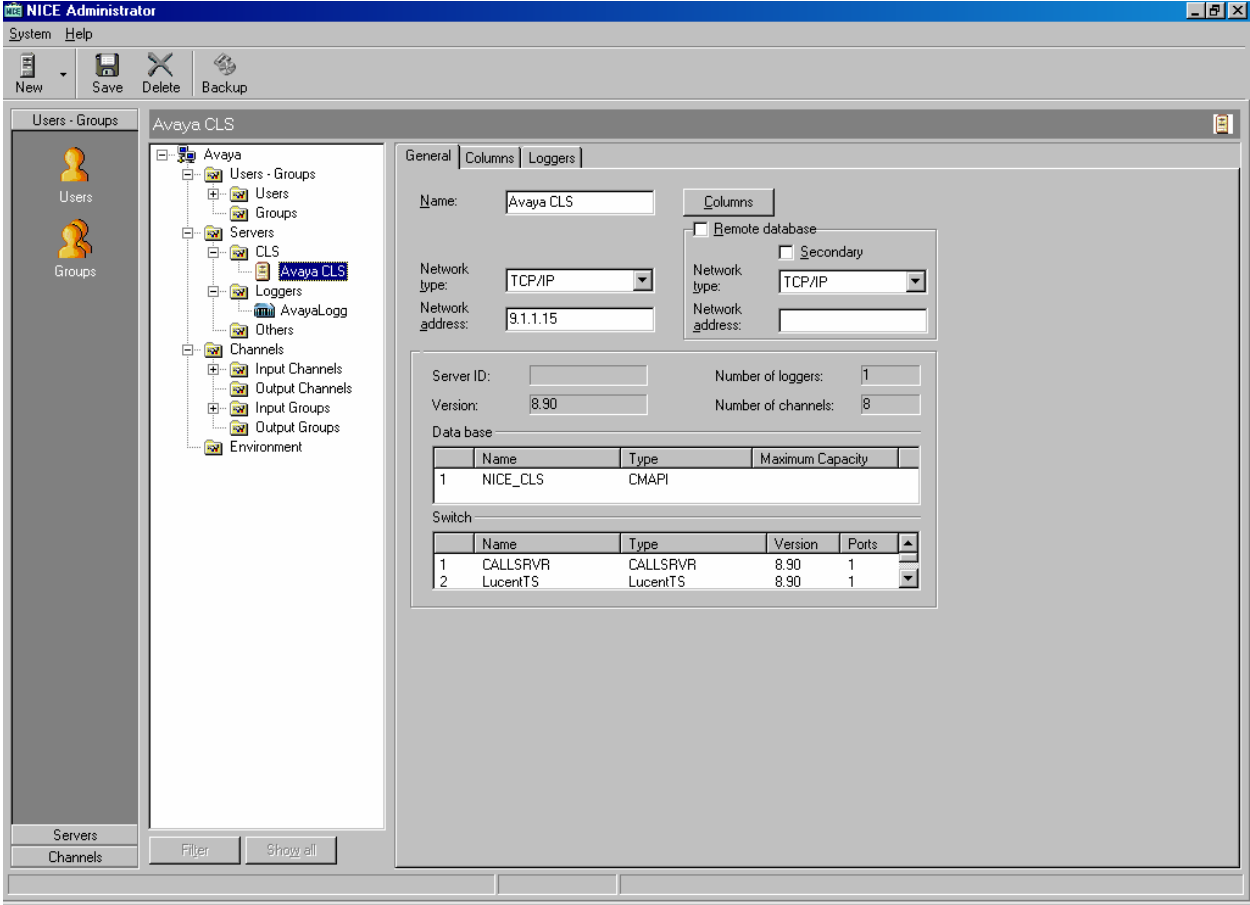
Step	Description
20.	<p>In the NiceCLS Server Controller, click on Server → Run NICE CLS.</p> <p>This will start the CLS Manager and the following screen will appear.</p> 

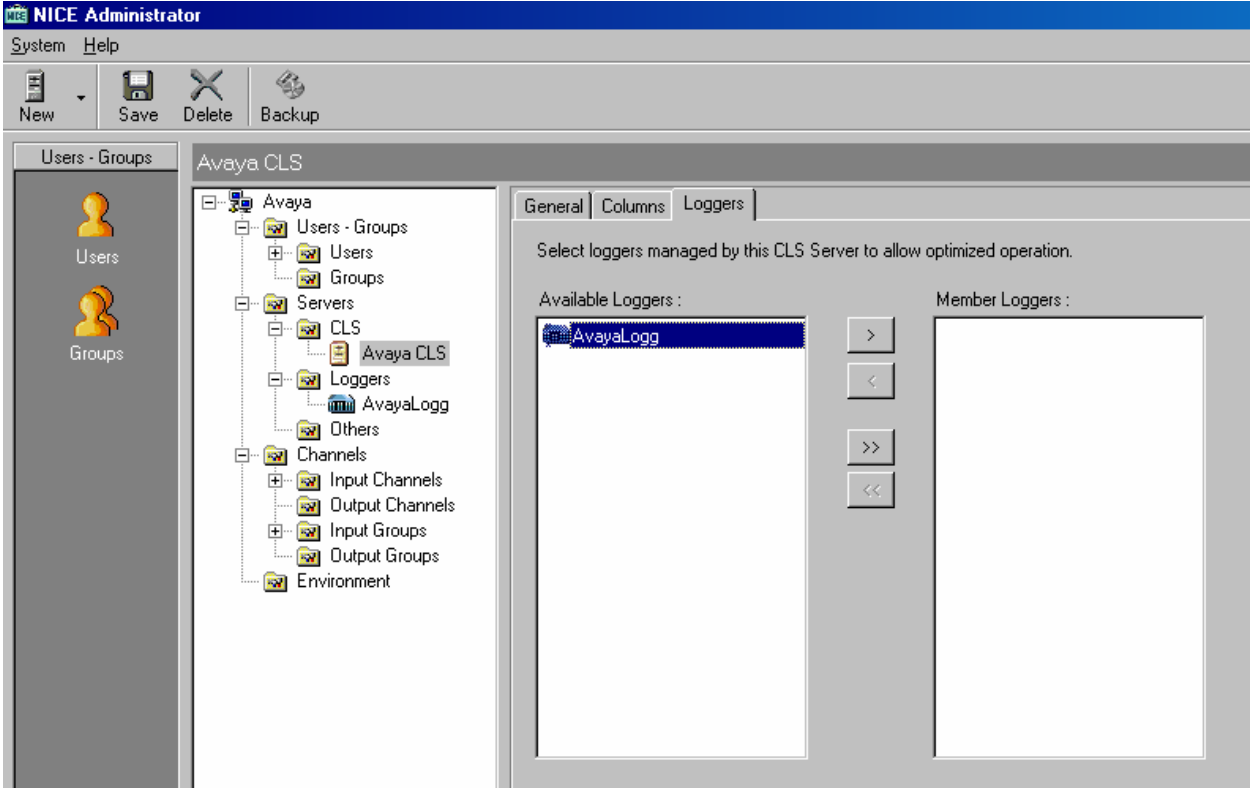
6.2. Configure the NICE Application Tools

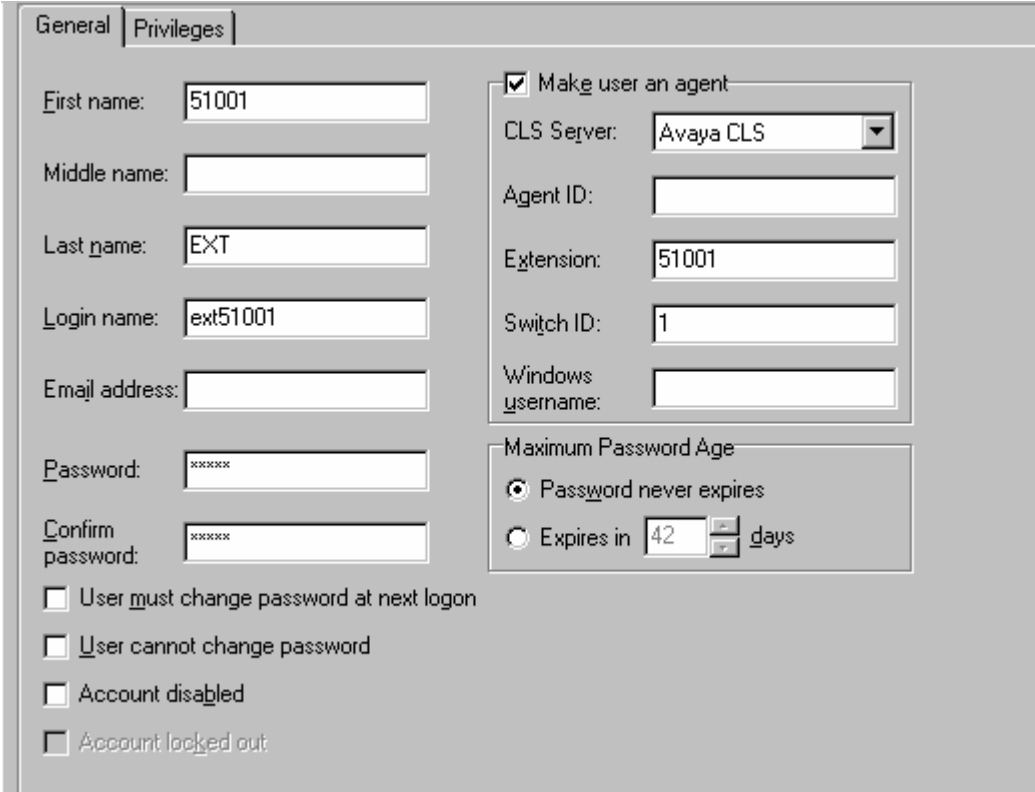
This section describes the steps necessary to configure the NICE Application Tools which include NICE Administrator, NICE Monitor and NICE Query. These client tools are used to manage NiceCLS and NiceLog. These Application Notes assume that the NICE Application Tools are already installed at the appropriate workstation.

Step	Description
1.	To start NICE Administrator, navigate to Programs → NICE Applications → NICE Administrator . Enter the proper credentials to log in.

Step	Description
2.	<p>In the NICE Administrator window, click New → NiceLog. The New NiceLog appears in the Resource List in the left panel. Click General tab, and enter the following values:</p> <ul style="list-style-type: none"> • Name: Enter a descriptive logger name, for example “AvayaLogg”. • Network type: Retain the default value “TCP/IP”. • Network address: Enter the IP Address of the Logger. • For retrieval: Enable the checkbox. <p>  Click on  icon </p> <p>The updated screen is shown below:</p>  <p>Note: After the NICE Administrator system connects with the NiceLog, the system populates the NiceLog information.</p>

Step	Description
3.	<p>In the NICE Administrator window, click New → NiceCLS Server. The New CLS Server window appears in the general area. Enter the following values and then click on  icon.</p> <ul style="list-style-type: none"> • Name: Enter a descriptive name. • Network Type: Select “TCP/IP” from the drop down list. • Network address: Enter the network address of the NiceCLS server. <p>The updated screen is shown below:</p>  <p>Note: After the NICE Administrator system connects with the NiceCLS, the system populates the NiceCLS information.</p>

Step	Description
4.	<p>Click on Loggers tab. Move the Logger, administered in Step 2, from the Available Loggers list to the Member Logger list. Click Save.</p>  <p>The screenshot shows the NICE Administrator application window. The title bar reads 'NICE Administrator'. Below the title bar are menus for 'System' and 'Help'. A toolbar contains icons for 'New', 'Save', 'Delete', and 'Backup'. The main window is divided into a left sidebar and a main content area. The sidebar has a 'Users - Groups' section with icons for 'Users' and 'Groups'. The main content area is titled 'Avaya CLS' and has three tabs: 'General', 'Columns', and 'Loggers'. The 'Loggers' tab is active. It contains the instruction: 'Select loggers managed by this CLS Server to allow optimized operation.' Below this are two lists: 'Available Loggers' and 'Member Loggers'. The 'Available Loggers' list contains one item, 'AvayaLogg', which is highlighted. The 'Member Loggers' list is empty. Between the two lists are four buttons: '>', '<', '>>', and '<<'. The 'Avaya' tree structure is visible in the background of the main content area.</p>

Step	Description
5.	<p>In the NICE Administrator, click New → User. Enter the following values, and then click Save.</p> <ul style="list-style-type: none"> • First name: Enter a descriptive name. • Last name: Enter a descriptive name. • Login name: Enter login name. • Password: Enter the password that will be used by the NICE Application Tools. • User must change password at next logon: Disable the checkbox. • Make user an agent: Enable the checkbox. • CLS Server: Select the CLS Server administered in Step 3 from the drop down list. • Extension: Enter the station extension which will be monitored. • Switch ID: Enter “1”. <p>Repeat this step as necessary to add additional Users.</p> 
6.	To start NICE Query, navigate to Programs → NICE Applications → NICE Query . Enter the proper credentials to log in.
7.	<p>In the NICE Query, click New → Query. Enter the following values, and then click OK.</p> <ul style="list-style-type: none"> • Query name: Enter a descriptive name.

7. General Test Approach and Test Results

Feature functionality testing was performed manually. Call recording and playback was verified for incoming/outgoing calls. In addition, phone features like hold, conference calls and transfers were exercised while the call was being recorded.

8. Verification

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya Application Enablement Services, and NICE call recording application.

8.1. Verify Avaya Communication Manager

On Avaya Communication Manager, verify the status of the administered CTI links by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link numbers administered in **Section 4.6**, 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	govaes1	established	611	611
2	4	no	govaes2	established	611	611

Issue the **list registered-ip-stations** command from the Avaya Communication Manager SAT to verify the NiceLog recording channels are registered in Avaya Communication Manager

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

Page 1

REGISTERED IP STATIONS								
Station Ext/ Orig Port	Set Type	Product ID	Prod Rel	Station IP Address	Net Rgn	Gatekeeper IP Address	TCP Skt	
23001	4625	IP_Phone	2.8300	9.1.1.85	1	9.1.1.8	y	
40030	4621	IP_Phone	2.8000	9.1.1.153	1	9.1.1.8	y	
44000	4625	IP_Phone	2.6000	9.1.1.143	1	9.1.1.8	y	
44002	4625	IP_Phone	2.6000	9.1.1.177	1	9.1.1.9	y	
44004	4625	IP_Phone	2.6000	9.1.1.175	1	9.1.1.8	y	
46001	4624	IP_API_A	3.2040	9.1.1.51	1	9.1.1.8	y	
46002	4624	IP_API_A	3.2040	9.1.1.51	1	9.1.1.8	y	
46003	4624	IP_API_A	3.2040	9.1.1.51	1	9.1.1.8	y	
46004	4624	IP_API_A	3.2040	9.1.1.51	1	9.1.1.8	y	
46005	4624	IP_API_A	3.2040	9.1.1.51	1	9.1.1.8	y	
46006	4624	IP_API_A	3.2040	9.1.1.51	1	9.1.1.8	y	
46007	4624	IP_API_A	3.2040	9.1.1.51	1	9.1.1.8	y	
46008	4624	IP_API_A	3.2040	9.1.1.51	1	9.1.1.8	y	

8.2. Verify Avaya Application Enablement Services

On Avaya AES, verify the status of the switch connection by selecting **Status and Control > Switch Conn Summary** from the left pane. Verify that the **Conn State** is “Talking” for the switch connection administered in **Section 5.3**, as shown below.

The screenshot shows the Avaya AES interface. The left pane contains a navigation menu with the following items: CTI OAM Home, Administration, Status and Control (selected), Maintenance, Alarms, Logs, Utilities, and Help. Under Status and Control, the following sub-items are listed: Switch Conn Summary (selected), Services Summary, and Maintenance. The main pane displays the 'Switch Connections Summary' page. The breadcrumb trail is 'You are here: > Status and Control > Switch Conn Summary'. The page title is 'Switch Connections Summary'. Below the title is a table with the following columns: Switch Conn, Conn State, Since, Online/Offline, Active CLANs/Admin'd CLANs, # of TCI Conns, Msgs To Switch, Msgs From Switch, and Msg Period. The table contains one row for the switch 'govaes2' with the following values: Conn State is 'Talking', Since is '2009-01-21 11:05:42.0', Online/Offline is 'Online', Active CLANs/Admin'd CLANs is '2 / 2', # of TCI Conns is '2', Msgs To Switch is '1315', Msgs From Switch is '812', and Msg Period is '30'. Below the table are four buttons: 'Online', 'Offline', 'Message Period', and 'Switch Connection Details'. At the bottom of the page is a button labeled 'Per Service Switch Connections Details'.

Switch Conn	Conn State	Since	Online/Offline	Active CLANs/Admin'd CLANs	# of TCI Conns	Msgs To Switch	Msgs From Switch	Msg Period
govaes2	Talking	2009-01-21 11:05:42.0	Online	2 / 2	2	1315	812	30

Verify the status of the TSAPI link by selecting **Status and Control > Services Summary** from the left pane. Click on **TSAPI Service**, followed by **Details** (not shown below). The **TSAPI Link Details** screen is displayed. Verify the **Conn Status** is “Talking” for the TSAPI link administered in **Section 5.4**, as shown below.

The screenshot shows the Avaya AES interface. The left pane contains a navigation menu with the following items: CTI OAM Home, Administration, Status and Control (selected), Maintenance, Alarms, Logs, Utilities, and Help. Under Status and Control, the following sub-items are listed: Switch Conn Summary, Services Summary (selected), and Maintenance. The main pane displays the 'TSAPI Link Details' page. The breadcrumb trail is 'You are here: > Status and Control > Services Summary'. The page title is 'TSAPI Link Details'. Below the title is a table with the following columns: Link, Switch Conn Name, Switch CTI Link Number, Conn Status, Since, Service State, Switch Version, Number of Associations, and ASAI Message Rate. The table contains one row for the link '1' with the following values: Switch Conn Name is 'govaes2', Switch CTI Link Number is '2', Conn Status is 'Talking', Since is '2009-01-21 11:05:42.0', Service State is 'Online', Switch Version is '15', Number of Associations is '14', and ASAI Message Rate is '613'.

Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
1	govaes2	2	Talking	2009-01-21 11:05:42.0	Online	15	14	613

Verify the status of the DMCC by selecting **Status and Control > Services Summary** from the left pane. Click on **DMCC Service**, followed by **Details** (not shown below). The **DMCC Service Summary – Session Summary** screen is displayed. Verify the nice cmapi session is listed.

The screenshot shows the AVAYA Application Enablement Services (AES) interface. The left navigation pane includes links for CTI OAM Home, Administration, Status and Control (with sub-links for Switch Conn Summary and Services Summary), Maintenance, Alarms, Logs, Utilities, and Help. The main content area displays the 'DMCC Service Summary - Session Summary' page. It includes a breadcrumb trail: 'You are here: > Status and Control > Services Summary'. The page title is 'DMCC Service Summary - Session Summary'. Below the title, there are links for 'Session Summary' and 'Device Summary', and a timestamp: 'Generated on Tue, Jan 27, 2009 03:53:08 PM EST'. The summary statistics are: Service Uptime: 0 days, 0:06 hours; Number of Active Sessions: 1; Number of Sessions Created Since Service Boot: 1; Number of Existing Devices: 8; Number of Devices Created Since Service Boot: 60. A table lists the sessions with columns: Session ID, User, Application, Far-end Identifier, Connection Type, and # of Associated Devices. One session is listed with ID '92D93CF65FDCF10A5F9E058EF2920C7E-0', User 'nice', Application 'cmapiApplication', Far-end Identifier '9.1.1.15', Connection Type 'XML Unencrypted', and 8 associated devices. At the bottom, there are buttons for 'Terminate Sessions' and 'Show Terminated Sessions'.

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
92D93CF65FDCF10A5F9E058EF2920C7E-0	nice	cmapiApplication	9.1.1.15	XML Unencrypted	8

Select **Session Summary Device Summary**. The details of all the devices registered with NICE application will be displayed. These should match the “list registered-ip-stations” from **Section 8.1**.


The screenshot shows the AVAYA Application Enablement Services (AES) interface. The left navigation pane is the same as in the previous screenshot. The main content area displays the 'DMCC Service Summary - Device Summary' page. It includes a breadcrumb trail: 'You are here: > Status and Control > Services Summary'. The page title is 'DMCC Service Summary - Device Summary'. Below the title, there are links for 'Session Summary' and 'Device Summary', and a timestamp: 'Generated on Tue, Jan 27, 2009 03:54:18 PM EST'. The summary statistics are: Service Uptime: 0 days 0:07 hours; Number of Active Sessions: 1; Number of Sessions Created Since Service Boot: 1; Number of Existing Devices: 8; Number of Devices Created Since Service Boot: 74. A table lists the devices with columns: Device ID, State, and Associated Sessions. Eight devices are listed, all with State 'REGISTERED' and 1 associated session. At the bottom, there is a button for 'Terminate Devices'.

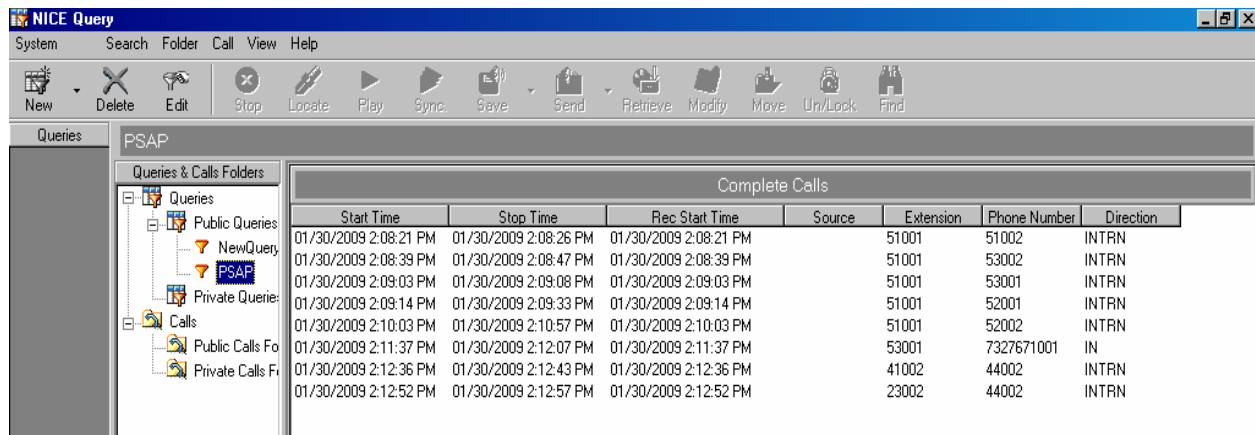
Device ID	State	Associated Sessions
46001:govaes2:9.1.1.8:0	REGISTERED	1
46002:govaes2:9.1.1.8:0	REGISTERED	1
46003:govaes2:9.1.1.8:0	REGISTERED	1
46004:govaes2:9.1.1.8:0	REGISTERED	1
46005:govaes2:9.1.1.8:0	REGISTERED	1
46006:govaes2:9.1.1.8:0	REGISTERED	1
46007:govaes2:9.1.1.8:0	REGISTERED	1
46008:govaes2:9.1.1.8:0	REGISTERED	1

8.3. Verify Call Recording and Playback from the NICE Query and Monitor

Make several calls. Verify that the recorded calls can be queried and playback from the NICE Query.



From the NICE Tool bar click on the NICE Query  icon and run query.



NICE Query

System Search Folder Call View Help

New Delete Edit Stop Locate Play Sync Save Send Retrieve Modify Move Un/Lock Find

Queries PSAP

Queries & Calls Folders

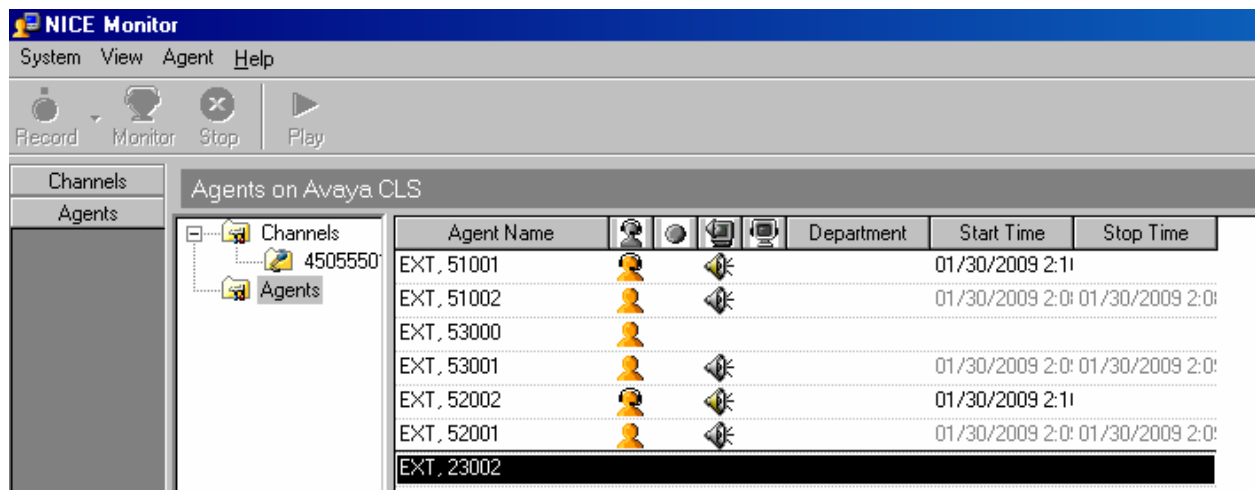
- Queries
 - Public Queries
 - NewQuery
 - PSAP
 - Private Queries
- Calls
 - Public Calls Folders
 - Private Calls Folders

Complete Calls

Start Time	Stop Time	Rec Start Time	Source	Extension	Phone Number	Direction
01/30/2009 2:08:21 PM	01/30/2009 2:08:26 PM	01/30/2009 2:08:21 PM		51001	51002	INTRN
01/30/2009 2:08:39 PM	01/30/2009 2:08:47 PM	01/30/2009 2:08:39 PM		51001	53002	INTRN
01/30/2009 2:09:03 PM	01/30/2009 2:09:08 PM	01/30/2009 2:09:03 PM		51001	53001	INTRN
01/30/2009 2:09:14 PM	01/30/2009 2:09:33 PM	01/30/2009 2:09:14 PM		51001	52001	INTRN
01/30/2009 2:10:03 PM	01/30/2009 2:10:57 PM	01/30/2009 2:10:03 PM		51001	52002	INTRN
01/30/2009 2:11:37 PM	01/30/2009 2:12:07 PM	01/30/2009 2:11:37 PM		53001	7327671001	IN
01/30/2009 2:12:36 PM	01/30/2009 2:12:43 PM	01/30/2009 2:12:36 PM		41002	44002	INTRN
01/30/2009 2:12:52 PM	01/30/2009 2:12:57 PM	01/30/2009 2:12:52 PM		23002	44002	INTRN



From the NICE Tool bar click on the NICE Monitor  icon.



NICE Monitor

System View Agent Help

Record Monitor Stop Play

Channels Agents

Agents on Avaya CLS

Agent Name	Department	Start Time	Stop Time
EXT, 51001		01/30/2009 2:11	
EXT, 51002		01/30/2009 2:01	01/30/2009 2:01
EXT, 53000			
EXT, 53001		01/30/2009 2:01	01/30/2009 2:01
EXT, 52002		01/30/2009 2:11	
EXT, 52001		01/30/2009 2:01	01/30/2009 2:01
EXT, 23002			

9. Terminology

AES	Avaya Application Enablement Services
ALI	Automatic Location Information
ANI	Automatic Number Identification
CAMA	Centralized Automated Message Accounting
DMCC	Device, Media and Call Control
IWS	Intelligent Workstation
NENA	National Emergency Number Association
PSAP	Public Safety Answering Point
SES	SIP Enablement Services
TSAPI	Telephony Services Application Programming Interface

10. Conclusion

These Application Notes demonstrate how to provision NICE Call Recording System for Public Safety which includes NICE CLS 8.90.4 and VoIP Logger 9.10.05 with Avaya Communication Manager, and Avaya Application Enablement Services to record and monitor incoming and outgoing calls on Avaya Communication Manager.

11. Additional References

1. *Application Enablement Services TSAPI, JTAPI and CVLAN Client and SDK Installation Guide*, Document 02-300543, May 2008, available at <http://support.avaya.com>.
2. *Application Enablement Services Administration and Maintenance Guide*, Document 02-300357, May 2008, available at <http://support.avaya.com>.
3. *NICE Administrator's Manual 8.*, available at <http://www.nice.com>
4. *Application Notes for PlantCML Sentinel CM with Avaya Communication Manager and Avaya Application Enablement Services.*
5. *Application Notes for Raytheon JPS ACU-2000IP with Avaya Communication Manager and Avaya SIP Enablement Services.*

©2009 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.